

# New Features Guide

**FortiAnalyzer 7.2.0**



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



March 21, 2023

FortiAnalyzer 7.2.0 New Features Guide

05-720-781586-20230321

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>Overview</b>	<b>6</b>
<b>Device Manager</b>	<b>7</b>
Device and Groups	7
Device Group	7
Support for six major versions of FortiOS 7.2.1	10
<b>Central Management</b>	<b>11</b>
Others	11
SAML SSO wildcard admin user to match all users on IdP server	11
<b>Security Fabric</b>	<b>14</b>
Others	14
OAuth 2.0 authentication for webhook connectors	14
<b>Security Operations (SOC)</b>	<b>16</b>
SOC automation	16
Use ServiceNow connector in playbooks	16
Incident and Event Management	18
Network reconnaissance events detection	18
Shadow IT events detection	22
New event handlers for NOC monitoring	25
Include IOC detected on FortiGate local traffic in FortiAnalyzer IOC view	27
Rule based event correlation 7.2.2	28
Data exfiltration detection 7.2.2	37
Dashboards	39
SD-WAN chart to include more ADVPN shortcut information	40
SD-WAN chart for MOS scoring	42
Add ZTNA dashboard to FortiView	46
IoT visibility	49
Traffic shaping charts 7.2.1	50
CASB Apps Access widget 7.2.1	53
Auto-refresh on FortiSoC dashboard elements 7.2.2	54
Others	55
Rename Outbreak Alerts Service to Outbreak Detection Service	55
<b>Log and Report</b>	<b>58</b>
Logging	58
Summary dashboard for event logs	58
Log caching enhancement	62
FortiNDR logging and reporting enhancements 7.2.1	64
Security events consolidated page 7.2.1	66
Reports	69
Report in JSON format	69
Report cache control	70
Upgrade report editor	71
Improve data visualization for the web usage report	74

360 Security Report .....	76
VPN report update 7.2.1 .....	78
Application risk and control report update 7.2.1 .....	82
Bandwidth and applications report update 7.2.1 .....	84
Security events and incidents summary report update 7.2.1 .....	85
High bandwidth application usage report update 7.2.1 .....	87
Cyber-bullying indicators report update 7.2.1 .....	89
Self-harm and risk indicators report update 7.2.2 .....	91
Others .....	93
Use device metadata in datasets and reports .....	93
Search by object names .....	95
Generate system event log when daemon crashes 7.2.2 .....	96
<b>System .....</b>	<b>98</b>
High Availability (HA) .....	98
Global log search across FortiAnalyzer Fabric members 7.2.1 .....	98
Administrators .....	101
Add French language support to GUI .....	101
Network .....	103
FortiAnalyzer supports VLANs on physical network interfaces .....	103
Others .....	105
FortiAnalyzer Fabric usability improvements .....	105
Add LLDP support on FMG and FAZ 7.2.1 .....	109
Mandatory FortiCare/FortiCloud registration 7.2.1 .....	109
<b>Cloud Services .....</b>	<b>111</b>
FortiAnalyzer management from FortiGate Cloud 7.2.1 .....	111
VM flexible shapes support for Oracle Cloud Infrastructure 7.2.1 .....	113
FortiAnalyzer-VM has been added to the Flex-VM offering 7.2.2 .....	115
FortiAnalyzer-VM supported in OCI DRCC 7.2.2 .....	116
<b>Index .....</b>	<b>117</b>
7.2.0 .....	117
7.2.1 .....	117
7.2.2 .....	118



# Change Log

Date	Change Description
2022-04-11	Initial release of FortiAnalyzer 7.2.0.
2022-04-20	Added <a href="#">SAML SSO wildcard admin user</a> to match all users on IdP server on page 11.
2022-04-25	Added: <ul style="list-style-type: none"><li>• <a href="#">Report cache control</a> on page 70</li><li>• <a href="#">Rename Outbreak Alerts Service to Outbreak Detection Service</a> on page 55</li><li>• <a href="#">FortiAnalyzer Fabric usability improvements</a> on page 105</li></ul>
2022-05-06	Added: <ul style="list-style-type: none"><li>• <a href="#">Add ZTNA dashboard to FortiView</a> on page 46</li><li>• <a href="#">Include IOC detected on FortiGate local traffic in FortiAnalyzer IOC view</a> on page 27</li></ul>
2022-06-06	Added: <ul style="list-style-type: none"><li>• <a href="#">IoT visibility</a> on page 49</li><li>• <a href="#">Upgrade report editor</a> on page 71</li></ul>
2022-08-09	Initial release of FortiAnalyzer 7.2.1.
2022-08-30	Added: <ul style="list-style-type: none"><li>• <a href="#">FortiNDR logging and reporting enhancements 7.2.1</a> on page 64</li><li>• <a href="#">Improve data visualization for the web usage report</a> on page 74</li><li>• <a href="#">VPN report update 7.2.1</a> on page 78</li></ul>
2022-08-31	Added: <ul style="list-style-type: none"><li>• <a href="#">Traffic shaping charts 7.2.1</a> on page 50</li><li>• <a href="#">Security events consolidated page 7.2.1</a> on page 66</li></ul>
2022-09-06	Added: <ul style="list-style-type: none"><li>• <a href="#">Application risk and control report update 7.2.1</a> on page 82</li><li>• <a href="#">Bandwidth and applications report update 7.2.1</a> on page 84</li><li>• <a href="#">Security events and incidents summary report update 7.2.1</a> on page 85</li><li>• <a href="#">High bandwidth application usage report update 7.2.1</a> on page 87</li><li>• <a href="#">Cyber-bullying indicators report update 7.2.1</a> on page 89</li></ul>
2022-09-20	Added: <ul style="list-style-type: none"><li>• <a href="#">FortiAnalyzer management from FortiGate Cloud 7.2.1</a> on page 111</li><li>• <a href="#">VM flexible shapes support for Oracle Cloud Infrastructure 7.2.1</a> on page 113</li></ul>
2022-11-08	Added <a href="#">CASB Apps Access widget 7.2.1</a> on page 53.
2023-02-02	Initial release of FortiAnalyzer 7.2.2.
2023-03-21	Added <a href="#">Mandatory FortiCare/FortiCloud registration 7.2.1</a> on page 109.

# Overview

This guide provides details of new features introduced in FortiAnalyzer 7.2. For each feature, the guide provides detailed information on configuration, requirements, and limitations, as applicable.

The FortiAnalyzer new features are organized into the following categories:

- [Device Manager on page 7](#)
- [Central Management on page 11](#)
- [Security Fabric on page 14](#)
- [Security Operations \(SOC\) on page 16](#)
- [Log and Report on page 58](#)
- [System on page 98](#)
- [Cloud Services on page 111](#)

For a list of all features organized by the version number that they were introduced, see [Index on page 117](#).

# Device Manager

This section lists the new features added to FortiAnalyzer for the device manager:

- [Device and Groups on page 7](#)

## Device and Groups

This section lists the new features added to FortiAnalyzer for devices and groups:

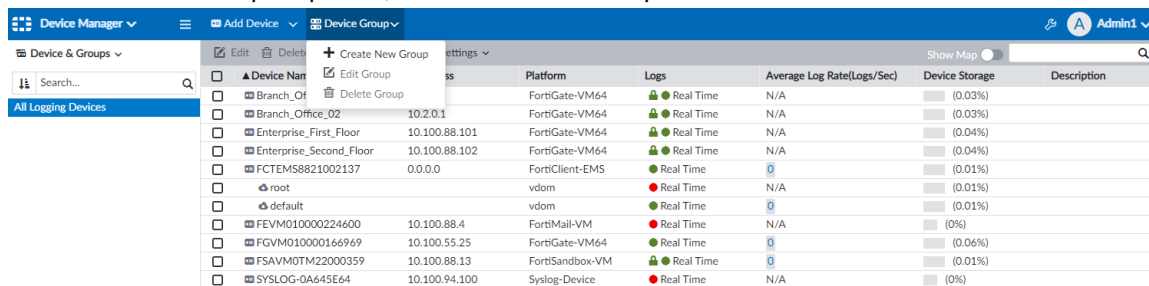
- [Device Group on page 7](#)
- [Support for six major versions of FortiOS 7.2.1 on page 10](#)

## Device Group

The FortiAnalyzer admin can create a device group and add devices to the group to simplify logging device management. The device group is automatically listed as a filter in Log View, FortiView and Reports device dropdown box for selection.

**To create a device group:**

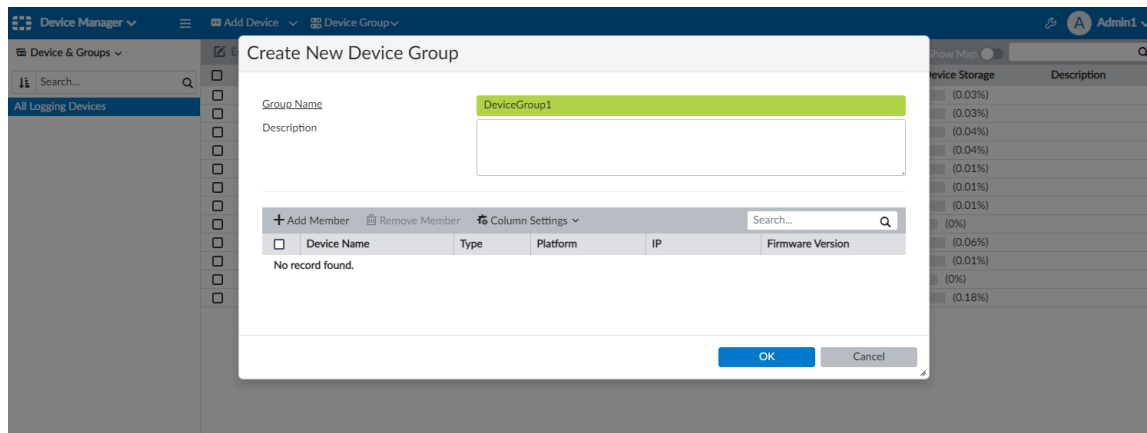
1. Go to *Device Manager*.
2. From the *Device Group* dropdown, click *Create New Group*.



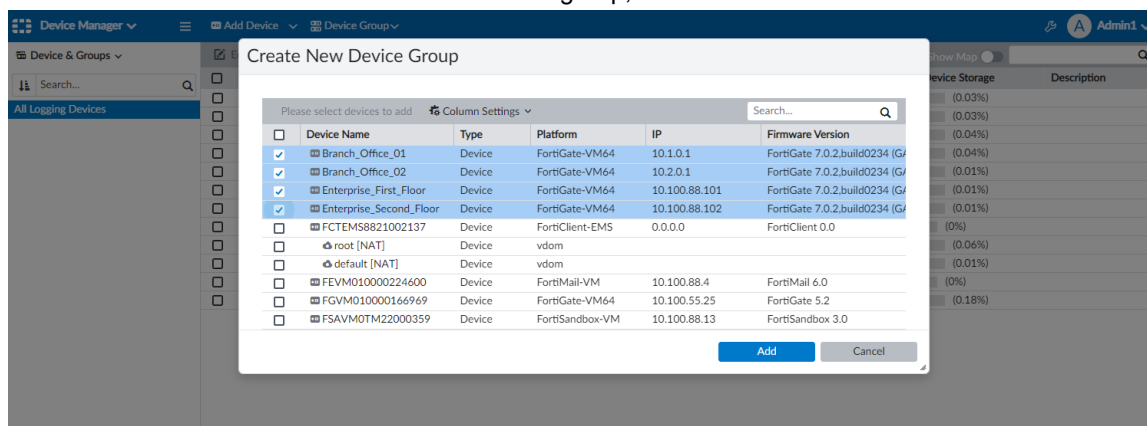
The *Create New Device Group* dialog opens.

3. In the *Group Name* field, type a name to identify the group of devices. *Description* is optional.

4. Click *Add Member* to view a list of devices.



5. Select the check box for each device to add to the group, and click *Add*.



6. Click *OK*.

The device group is now available. You can right-click the device group to edit or delete it.

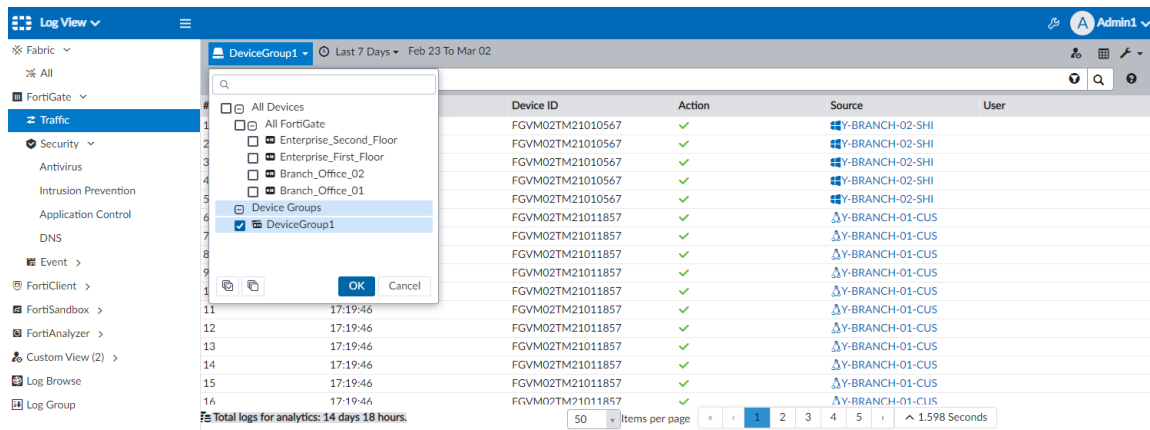


You cannot edit or delete the default device groups, such as the *All Logging Devices* device group.

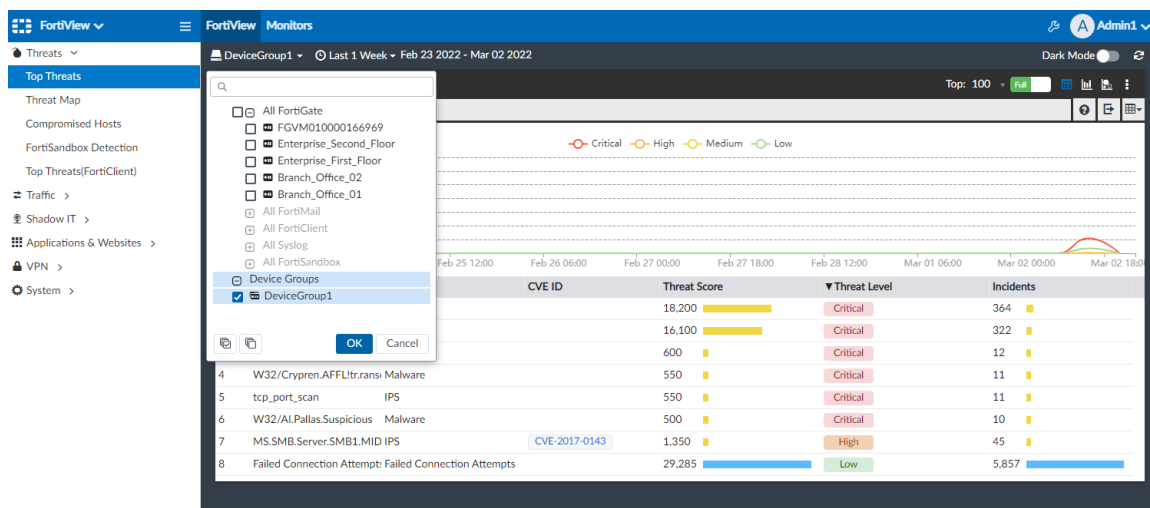
Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	Description
Branch_Office_01	10.1.0.1	FortiGate-VM64	Real Time	N/A	(0.03%)	
Branch_Office_02	10.2.0.1	FortiGate-VM64	Real Time	N/A	(0.03%)	
Enterprise_First_Floor	10.100.88.101	FortiGate-VM64	Real Time	N/A	(0.04%)	
Enterprise_Second_Floor	10.100.88.102	FortiGate-VM64	Real Time	N/A	(0.04%)	

This device group can now be used in *Log View*, *FortiView*, event handlers, and *Reports*. See examples below with DeviceGroup1 as the device group.

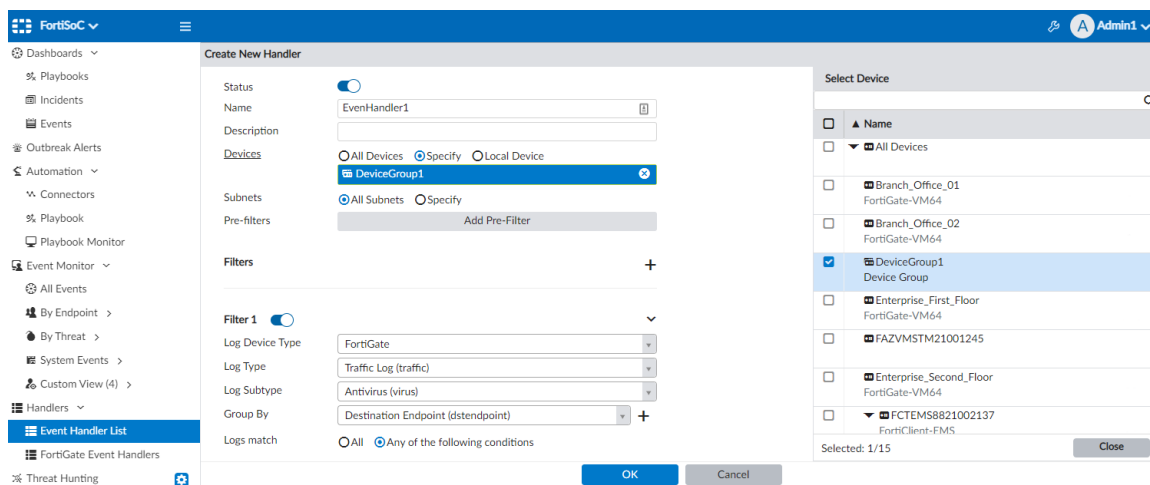
Filtering *Log View > FortiGate > Traffic* by the device group:



Filtering *FortiView > Threats > Top Threats* by the device group:

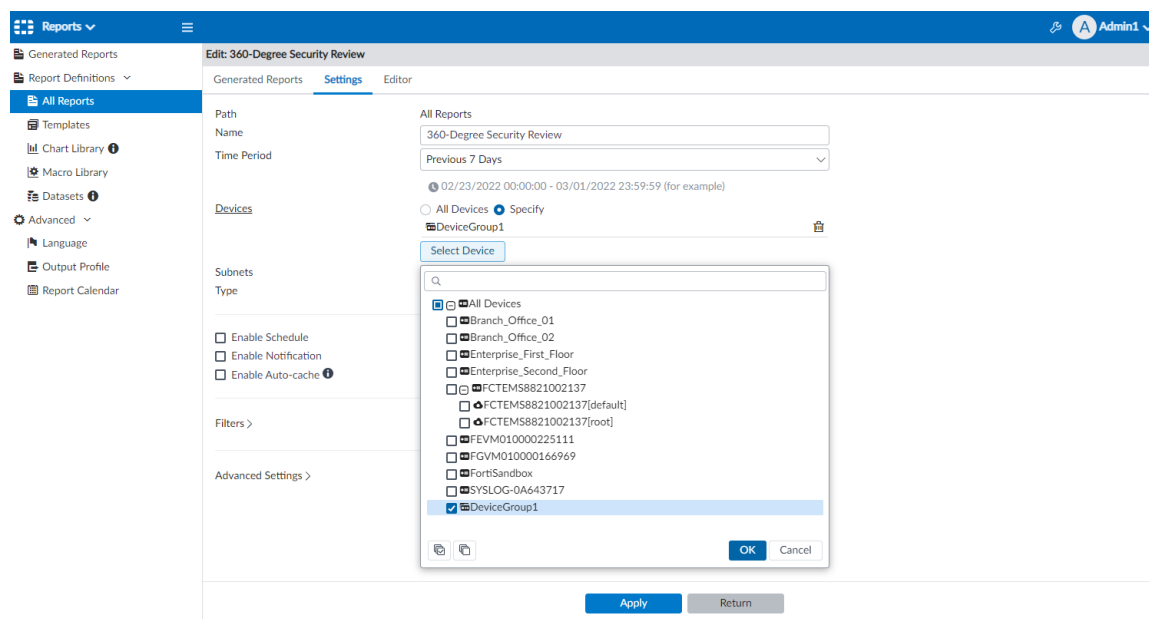


Using the device group for an event handler:



Using the device group in *Reports*:





## Support for six major versions of FortiOS - 7.2.1

FortiAnalyzer 7.2.1 and later supports six major versions of FortiOS to let you access to all the features and enhancements of the latest FortiAnalyzer firmware without upgrading your FortiGates to later versions of FortiOS. For example, FortiAnalyzer 7.2.1 supports the following major versions of FortiOS:

- 7.2
- 7.0
- 6.4
- 6.2
- 6.0
- 5.6

For information about supported models for each major FortiOS version, see the [FortiAnalyzer 7.2.1 Release Notes](#).

# Central Management

This section lists the new features added to FortiAnalyzer for central management:

- [Others on page 11](#)

## Others

This section lists the new features added to FortiAnalyzer for other topics relating to central management:

- [SAML SSO wildcard admin user to match all users on IdP server on page 11](#)

## SAML SSO wildcard admin user to match all users on IdP server

In FortiAnalyzer 7.2.0, you can create a SAML SSO wildcard admin user to match all users on the IdP server.

In the following examples, the IdP is configured with the following local users and profiles:

- *test1* is configured with profile1 which specifies access to adom1.
- *test2* is configured with profile2 which specifies access to adom2.
- *test3* is configured with profile3 which specifies access to all ADOMs.

As long as the SP has the same user profile and ADOM names as the IdP, when logging in as an SSO user on the SP, the user is assigned the same profile and ADOMs.

This example assumes that you have already configured SAML SSO in your environment.

### To configure a SAML wildcard user with SAML attributes:

1. On the SAML Identity Provider (IdP), click *Create New* under *SP Settings* to configure the service provider.
2. Attributes for the service provider can be added by clicking *Create New* under *SAML Attributes*.  
In this example, the following SAML attributes are used:

- Name: username, Type: Username
- Name: adom, Type: ADOM

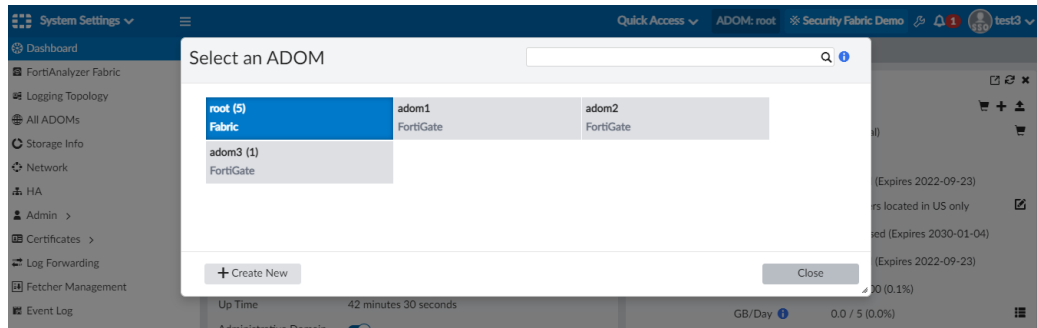
- Name: profile, Type: Profile Name

3. On the SAML Service Provider (SP), create one SAML SSO user and enable the *Match all users on remote server* option.

4. Log in to the SP as a local user created on the IdP.  
For example, the local users "test1", "test2", and "test3" have been created on the IdP.

Name	Type	Profile	JSON API Access	ADOMs
admin	LOCAL	Super_User	Read & Write	All ADOMs
test1	LOCAL	profile1	None	adom1
test2	LOCAL	profile2	None	adom2
test3	LOCAL	profile3	None	All ADOMs
test3	LOCAL	profile3	None	All ADOMs

When logging on to the SP as user "test3", the account has the same ADOM access settings as are configured for local user "test3" on the IdP.



# Security Fabric

This section lists the new features added to FortiAnalyzer for Security Fabric:

- [Others on page 14](#)

## Others

This section lists the new features added to FortiAnalyzer for other topics relating to Security Fabric:

- [OAuth 2.0 authentication for webhook connectors on page 14](#)

## OAuth 2.0 authentication for webhook connectors

OAuth 2.0 is now available for webhook connectors to provide simple, consistent, and secure authentication.

### To configure OAuth 2.0 for a webhook connector:

1. Go to *Fabric View > Fabric > Connectors*, and click *Create New*.
2. Under the *ITSM* category, click *Generic Connector*.  
You can also configure OAuth 2.0 authentication for an existing webhook connector by selecting the connector and clicking *Edit*.
3. Configure the following properties:

<b>Name</b>	Type a name for the connector.
<b>Description</b>	(Optional) Type a description for the connector.
<b>Protocol</b>	Select the protocol FortiAnalyzer uses to communicate with the external platform.
<b>Port</b>	Type the port FortiAnalyzer uses to communicate with the external platform.
<b>Method</b>	
<b>Title</b>	Type a title for the connector.
<b>URL</b>	Type the URL of the external platform.
<b>Enable HTTP Authentication</b>	Set HTTP authentication to <i>ON</i> .
<b>Auth Type</b>	Select <i>OAuth2</i> .
<b>Authorization Server</b>	Type the URL of the token service. The token service must be publicly available.
<b>Auth Client ID</b>	Type the client ID from the token service.
<b>Auth Client Secret</b>	Type the client secret from the token service.



**Status**Set status to *ON* to enable the fabric connector.**4. Click OK.**

Backend OAuth 2.0 libraries in FortiAnalyzer connect to the token service and authenticate with the provided client ID and client secret. When authentication is successful, FortiAnalyzer receives a token with a TTL and scope attached to it. FortiAnalyzer will use this token for all webhook connections to the token service until TTL expires.

The screenshot shows the 'Create New Fabric Connector' dialog box in the FortiAnalyzer web interface. The dialog is titled 'Create New Fabric Connector' and has a 'Generic Connector' icon. The fields are as follows:

- Name: Connector
- Description: (empty)
- Protocol: HTTP (selected), HTTPS
- Port: 80
- Method: POST (selected), PUT
- Title: Connector
- URL: 10.2.125.230:9096/webhook
- Enable HTTP Authentication: (checked)
- Auth Type: Basic, OAuth2 (selected)
- Authorization Server: http://10.2.125.230:9096/oauth/token
- Auth Client ID: qa
- Auth Client Secret: (masked with dots)
- Status: (checked)

The background shows the FortiAnalyzer interface with the 'Connectors' tab selected. The 'Security Fabric (3)' section is visible, showing 'FortiClient EMS' and 'EMS Connector FortiDemo'.

# Security Operations (SOC)

This section lists the new features added to FortiAnalyzer for security operations (SOC):

- [SOC automation on page 16](#)
- [Incident and Event Management on page 18](#)
- [Dashboards on page 39](#)
- [Others on page 55](#)

## SOC automation

This section lists the new features added to FortiAnalyzer for SOC automation:

- [Use ServiceNow connector in playbooks on page 16](#)

### Use ServiceNow connector in playbooks

ServiceNow Connector is supported by playbooks for more automation with ServiceNow integration. Playbooks can automatically create, update or delete Incident records in ServiceNow via the connector.

The incident trigger includes update/create/delete notices when connected to ServiceNow connector. For update notices, ServiceNow will refetch that incident to update the corresponding fields mapped to ServiceNow.



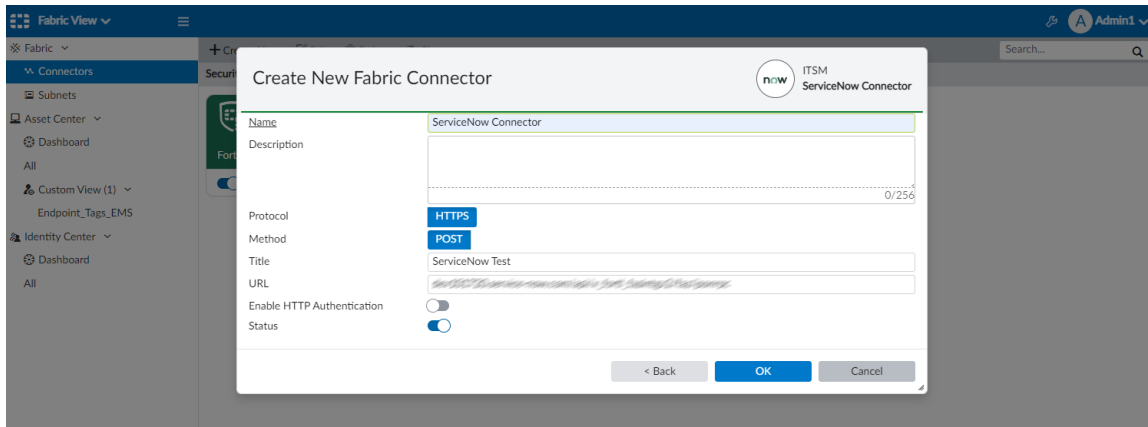
The ServiceNow instance must be running for the playbook to post incident change notices to the ServiceNow table. They will not post if the ServiceNow instance is hibernating.

---

#### To create the ServiceNow fabric connector:

1. Go to *Fabric View > Fabric > Connectors*, and click *Create New*.
2. In the *ITSM* category, click *ServiceNow Connector*.

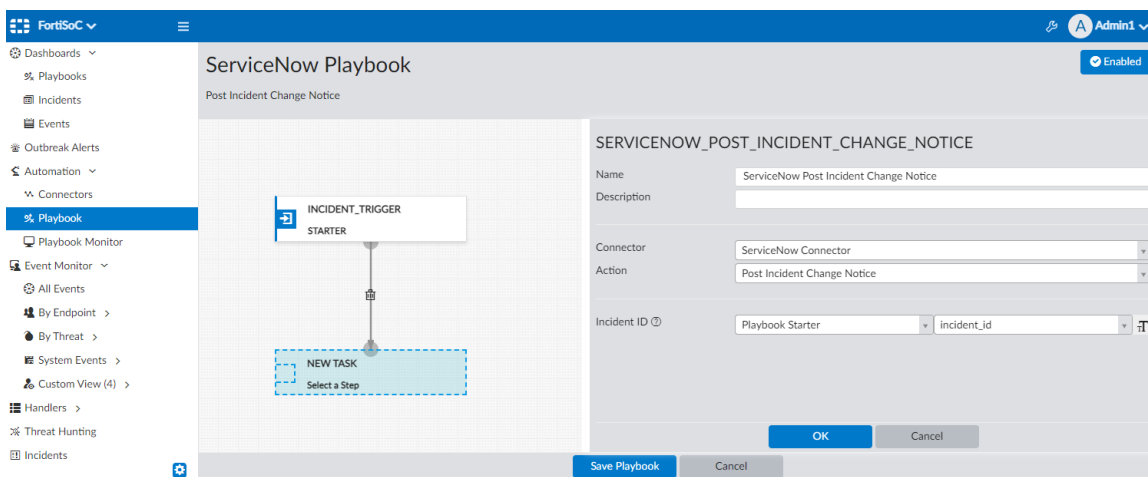
### 3. Configure the connector, and click **OK**.



### To create a playbook using the ServiceNow fabric connector:

1. Go to **FortiSoC > Automation > Playbook**, and click **Create New**.
2. From the list of playbook templates, select **New playbook created from scratch**. You can also edit an existing playbook according to your needs.
3. Click within the playbook's title fields to change its name and description.
4. Select a trigger for the playbook.
5. Configure the trigger's filter conditions, and click **OK**.
6. Drag a highlighted connector from the trigger to add a new step in the playbook.
7. From the list of connectors for the step, select **ServiceNow**.
8. Configure the step in the playbook, and click **OK**.

<b>Name</b>	Type a name for the step.
<b>Description</b>	(Optional) Type a description for the step.
<b>Connector</b>	Select the ServiceNow connector that you configured.
<b>Action</b>	Select <i>Post Incident Change Notice</i> .
<b>Incident ID</b>	Select <i>Playbook Starter</i> , <i>incident_id</i> .



### 9. Click **Save Playbook**.

## Incident and Event Management

This section lists the new features added to FortiAnalyzer for incident and event management:

- [Network reconnaissance events detection on page 18](#)
- [Shadow IT events detection on page 22](#)
- [New event handlers for NOC monitoring on page 25](#)
- [Include IOC detected on FortiGate local traffic in FortiAnalyzer IOC view on page 27](#)
- [Rule based event correlation 7.2.2 on page 28](#)
- [Data exfiltration detection 7.2.2 on page 37](#)

### Network reconnaissance events detection

A new factory default event handler is available to detect network reconnaissance activities from attackers. This event handler has 11 filters and is enabled by default.

**To view the network reconnaissance events handler:**

1. Go to *FortiSoC > Handlers > Event Handler List*.

The *Default-Recon-Activity-By-Endpoint* event handler is enabled by default.

Status	Name	Filters	Devices	Send Alert to	Events	Included Subnets	Excluded Subnets
<input checked="" type="checkbox"/>	Default-Recon-Activity-By-Endpoint	> 11 Filters	All Devices		12		
<input type="checkbox"/>	Local Device Event	> 1 Filter	Local Device		24		
<input type="checkbox"/>	Default-Botnet-Communication-Detection	> 9 Filters	All Devices				
<input type="checkbox"/>	Default-Compromised Host-Detection	> 3 Filters	All Devices				
<input type="checkbox"/>	Default-Malicious-Code-Detection-By-Endpoint	> 8 Filters	All Devices				
<input type="checkbox"/>	Default-Risky-Destination-Detection-By-Endpoint	> 15 Filters	All Devices		9		
<input type="checkbox"/>	Default-Risky-App-Detection-By-Threat	> 2 Filters	All Devices				
<input type="checkbox"/>	Default-Malicious-File-Detection-By-Threat	> 8 Filters	All Devices				
<input type="checkbox"/>	Default-Risky-App-Detection-By-Endpoint	> 4 Filters	All Devices				
<input type="checkbox"/>	Default-Malicious-File-Detection-By-Endpoint	> 24 Filters	All Devices				
<input type="checkbox"/>	Default-Malicious-Code-Detection-By-Endpoint	> 8 Filters	All Devices				
<input type="checkbox"/>	Default-Risky-Destination-Detection-By-Endpoint	> 14 Filters	All Devices		4		
<input type="checkbox"/>	Default-Compromised Host-Detection-IOC-By-Endpoint	> 3 Filters	All Devices				
<input type="checkbox"/>	Default-Botnet-Communication-Detection-By-Endpoint	> 9 Filters	All Devices				
<input type="checkbox"/>	Default-FFW System Events	> 8 Filters	All Devices				
<input type="checkbox"/>	Default-FFW-Compromised Host-Detection-IOC-By-Threat	> 3 Filters	All Devices				
<input type="checkbox"/>	Default-FFW-Risky-Destination-Detection-By-Threat	> 10 Filters	All Devices				
<input type="checkbox"/>	Default-FFW-Risky-Destination-Detection-By-Endpoint	> 10 Filters	All Devices				
<input type="checkbox"/>	Default-FFW-Compromised Host-Detection-IOC-By-Endpoint	> 2 Filters	All Devices				
<input type="checkbox"/>	Default-FFW-Botnet-Communication-Detection-By-Endpoint	> 1 Filter	All Devices				
<input type="checkbox"/>	Default-FFW-Threat-Detection-By-Hostname	> 4 Filters	All Devices				

19



Edit Handler: Default-Recon-Activity-By-Endpoint

Filter 5

Log Device Type: FortiGate

Log Type: Traffic Log (traffic)

Log Subtype: Any

Group By: Source Endpoint (endpoint)

Destination Port (dstport)

Logs match: All

Log Field: Service (service) Equal To DNS

Generic Text Filter: action=client-rst or action=timeout or action=deny and srcintfrole=wan and dstintfrole=wan

Generate Alert When: At least 300 over a period of 1440 minutes

Event Type Override: Specify an event type, or leave blank to use default value

Event Message: IP scanning on Port: \$groupby2 detected

Event Status: Unhandled

Event Severity: Medium

Tags: Risky Recon DNS

Indicators: Log Field No Indicator

Additional Info: Recon activity from: \$srcip:\$srcport to \$dstip:\$dstport

Edit Handler: Default-Recon-Activity-By-Endpoint

Filter 6

Log Device Type: FortiGate

Log Type: Traffic Log (traffic)

Log Subtype: Any

Group By: Source Endpoint (endpoint)

Destination Port (dstport)

Logs match: All

Log Field: Service (service) Equal To LDAP

Generic Text Filter: action=client-rst or action=timeout or action=deny and srcintfrole=wan and dstintfrole=wan

Generate Alert When: At least 35 over a period of 1440 minutes

Event Type Override: Specify an event type, or leave blank to use default value

Event Message: IP scanning on Port: \$groupby2 detected

Event Status: Unhandled

Event Severity: Medium

Tags: Risky Recon LDAP

Indicators: Log Field No Indicator

Additional Info: Recon activity from: \$srcip:\$srcport to \$dstip:\$dstport

Edit Handler: Default-Recon-Activity-By-Endpoint

Filter 7

Log Device Type: FortiGate

Log Type: Traffic Log (traffic)

Log Subtype: Any

Group By: Source Endpoint (endpoint)

Logs match: All

Log Field: Service (service) Equal To SMB

Generic Text Filter: action=client-rst or action=timeout or action=deny and srcintfrole=wan and dstintfrole=wan and service=icmp

Generate Alert When: At least 200 over a period of 1440 minutes

Event Type Override: Specify an event type, or leave blank to use default value

Event Message: IP scanning on source endpoint: \$groupby1 detected

Event Status: Unhandled

Event Severity: Medium

Tags: Risky Recon ICMP

Indicators: Log Field No Indicator

Additional Info: Recon activity from: \$srcip detected

Edit Handler: Default-Recon-Activity-By-Endpoint

Filter 8

Log Device Type: FortiGate

Log Type: Traffic Log (traffic)

Log Subtype: Any

Group By: Source Endpoint (endpoint)

Destination Port (dstport)

Logs match: All

Log Field: Service (service) Equal To SMB

Generic Text Filter: action=client-rst or action=timeout or action=deny and srcintfrole=wan and dstintfrole=wan

Generate Alert When: At least 50 over a period of 1440 minutes

Event Type Override: Specify an event type, or leave blank to use default value

Event Message: IP scanning on Port: \$groupby2 detected

Event Status: Unhandled

Event Severity: Medium

Tags: Risky Recon SMB

Indicators: Log Field No Indicator

Additional Info: Recon activity from: \$srcip:\$srcport to \$dstip:\$dstport

Edit Handler: Default-Recon-Activity-By-Endpoint

Filter 9

Log Device Type  
FortiGate

Log Type  
Traffic Log (traffic)

Log Subtype  
Any

Group By  
Source Endpoint (endpoint)

Destination Port (dstport)

Logs match  
☒ All ☐ Any of the following conditions

Log Field  

Log Field	Match Criteria	Value
Service (service)	Equal To	SNMP

Generic Text Filter  

(action=client-rst or action=timeout or action=deny) and srcintrole=wan and dstintrole=wan

94/1023

Generate Alert When  
At least 150 over a period of 1440 minutes Destination IP (dstip) matches occurred

Event Type Override  
Specify an event type, or leave blank to use default value

Event Message  
IP scanning on Port: \$groupby2 detected

Event Status  
Unhandled

Event Severity  
Medium

Tags  
Risky Recon SNMP

Indicators  

Log Field	Indicator Type	Count
No Indicator		

Additional Info  
☐ Use system default  
☒ Use custom message  

Recon activity from: \$(srcip)\$(srcport) to \$(dstip)\$(dstport)

63/255

Edit Handler: Default-Recon-Activity-By-Endpoint

Filter 10

Log Device Type  
FortiGate

Log Type  
Traffic Log (traffic)

Log Subtype  
Any

Group By  
Source Endpoint (endpoint)

Destination Port (dstport)

Logs match  
☒ All ☐ Any of the following conditions

Log Field  

Log Field	Match Criteria	Value
Service (service)	Equal To	SMTP

Generic Text Filter  

(action=client-rst or action=timeout or action=deny) and srcintrole=wan and dstintrole=wan

94/1023

Generate Alert When  
At least 21 over a period of 1440 minutes Destination IP (dstip) matches occurred

Event Type Override  
Specify an event type, or leave blank to use default value

Event Message  
IP scanning on Port: \$groupby2 detected

Event Status  
Unhandled

Event Severity  
Medium

Tags  
Risky Recon SMTP

Indicators  

Log Field	Indicator Type	Count
No Indicator		

Additional Info  
☐ Use system default  
☒ Use custom message  

Recon activity from: \$(srcip)\$(srcport) to \$(dstip)\$(dstport)

63/255

Edit Handler: Default-Recon-Activity-By-Endpoint

Filter 11

Log Device Type  
FortiGate

Log Type  
Traffic Log (traffic)

Log Subtype  
Any

Group By  
Source Endpoint (endpoint)

Destination Port (dstport)

Logs match  
☒ All ☐ Any of the following conditions

Log Field  

Click to add

Generic Text Filter  

(service=rpc or app=rpc) and (action=client-rst or action=timeout or action=deny) and srcintrole=wan and dstintrole=wan

123/1023

Generate Alert When  
At least 10 over a period of 1440 minutes Destination IP (dstip) matches occurred

Event Type Override  
Specify an event type, or leave blank to use default value

Event Message  
IP scanning on Port: \$groupby2 detected

Event Status  
Unhandled

Event Severity  
Medium

Tags  
Risky Recon RPC

Indicators  

Log Field	Indicator Type	Count
No Indicator		

Additional Info  
☐ Use system default  
☒ Use custom message  

Recon activity from: \$(srcip)\$(srcport) to \$(dstip)\$(dstport)

63/255

## To view events generated by the recon activity handler:

1. Go to **FortiSoC > Event Monitor > All Events**.
2. Filter by **Handler = Default-Recon-Activity-By-Endpoint**.

#	Event	Additional Info	Event Type	Count	Severity	Handler	Tags
1	~172.18.25.168 (1)	Recon activity from: 172.18.25.168-46982 to 192.168.1.177...111	Traffic	14	Medium	Default-Recon-Activity-By-En...	Risky Recon RPC
2	~192.168.50.20 (9)	Recon activity from: 192.168.50.20-49234... to 8.8.8.10...21	Traffic	17	Medium	Default-Recon-Activity-By-En...	Risky Recon FTP
	IP scanning on Port: 21 detected	Recon activity from: 192.168.50.20-47404... to 8.8.8.10...25	Traffic	49	Medium	Default-Recon-Activity-By-En...	Risky Recon SMTP
	IP scanning on Port: 161 detected	Recon activity from: 192.168.50.20-52576... to 8.8.8.152...161	Traffic	221	Medium	Default-Recon-Activity-By-En...	Risky Recon SNMP
	IP scanning on Port: 53 detected	Recon activity from: 192.168.50.20-56298... to 4.2.2.107...53	Traffic	302	Medium	Default-Recon-Activity-By-En...	Risky Recon DNS
	IP scanning on Port: 445 detected	Recon activity from: 192.168.50.20-57402... to 8.8.8.55...445	Traffic	234	Medium	Default-Recon-Activity-By-En...	Risky Recon SMB
	IP scanning on Port: 389 detected	Recon activity from: 192.168.50.20-42246... to 8.8.8.35...389	Traffic	192	Medium	Default-Recon-Activity-By-En...	Risky Recon LDAP
	IP scanning on Port: 443 detected	Recon activity from: 192.168.50.20-32852... to 8.8.8.31...443	Traffic	210	Medium	Default-Recon-Activity-By-En...	Risky Recon HTTPS
	IP scanning on Port: 3389 detected	Recon activity from: 192.168.50.20-48268... to 8.8.8.15...3389	Traffic	149	Medium	Default-Recon-Activity-By-En...	Risky Recon RDP
	IP scanning on Port: 22 detected	Recon activity from: 192.168.50.20-33238... to 8.8.8.135...22	Traffic	222	Medium	Default-Recon-Activity-By-En...	Risky Recon SSH
3	~192.168.50.20 (1)	Recon activity from: 192.168.50.20-49214... to 8.8.8.10...21	Traffic	40	Medium	Default-Recon-Activity-By-En...	Risky Recon FTP
4	~172.17.97.21 (1)	Recon activity from: 172.17.97.21 detected	Traffic	440	Medium	Default-Recon-Activity-By-En...	Risky Recon ICMP

## Shadow IT events detection

A new factory default event handler is available to detect shadow IT events. These events include:

- High-risk unsanctioned cloud applications
- Unsanctioned users
- File exfiltration

To detect these events, FortiAnalyzer must be connected with the FortiCASB connector and running the *Get Cloud Service Data (FortiCasb Connector)* playbook. FortiAnalyzer applies the meta-data of sanctioned applications and sensitive files against the application control logs. Events are generated when these incoming application control logs meet the filter criteria of the *Default-Shadow-IT-Events* event handler.

**Edit Handler: Default-Shadow-IT-Events**

Filters (3)

**Filter 1** ☒ **Log Device Type** FortiGate

**Log Type** Application Control (app-ctrl)

**Group By** Source IP (srcip)

**Logs match** ☒ All ☐ Any of the following conditions

**Log Field** Match Criteria Value

**Click to add**

**Generic Text Filter** ☒ (srcip & 1) == 0 && slappid == 0

**Generate Alert When** At least 1 Exact matches occurred over a period of 1440 minutes

**Event Type Override** Specify an event type, or leave blank to use default value

**Event Message** Unsanctioned Applications detected

**Event Status** Unhandled

**Event Severity** High

**Tags** Unsanctioned\_App

**Indicators** Log Field Indicator Type Count

**Additional Info** ☒ Use system default ☐ Use custom message

Unsanctioned application \$[app] with app risk: \$[apprisk] detected on: \$[devname] with message: \$[msg]

**Filter 2** ☒ **Log Device Type** FortiGate

**Log Type** Application Control (app-ctrl)

**Group By** Source IP (srcip)

**Logs match** ☒ All ☐ Any of the following conditions

**Log Field** Match Criteria Value

**Click to add**

**Generic Text Filter** ☒ (srcip & 4) == 4

**Generate Alert When** At least 1 Exact matches occurred over a period of 1440 minutes

**Event Type Override** Specify an event type, or leave blank to use default value

**Event Message** File Exfiltration Attempts detected

**Event Status** Unhandled

**Event Severity** High

**Tags** File\_Exfiltration

**Indicators** Log Field Indicator Type Count

**Additional Info** ☒ Use system default ☐ Use custom message

File exfiltration detected on: \$[devname] with message: \$[msg]

**Edit Handler: Default-Shadow-IT-Events**

Filter 3 ☒ ⌵

Log Device Type: FortiGate

Log Type: Application Control (app-ctrl)

Group By: Source IP (srcip)

Application Name (app)

Logs match: ☒ All ☐ Any of the following conditions

Log Field	Match Criteria	Value
<a href="#">Click to add</a> <span>+</span> <span>⌵</span>		

Generic Text Filter ⓘ: (siflags & 1) == 1 && (siflags & 2) == 0 40/1023

Generate Alert When: At least   matches occurred over a period of  minutes

Event Type Override: Specify an event type, or leave blank to use default value

Event Message ⓘ: Unsanctioned Users detected

Event Status: Unhandled ⌵

☐ Allow FortiAnalyzer to choose

Event Severity: High ⌵

Tags: Unsanctioned\_User

Indicators:

Log Field	Indicator Type	Count
No Indicator		

[Additional Info](#)

☐ Use system default

☒ Use custom message ⓘ

Unsanctioned user: \${unauthuser} with app risk: \${apprisk} detected on: \${devname} with message: \${msg} 103/255

### To enable the shadow IT event handler:

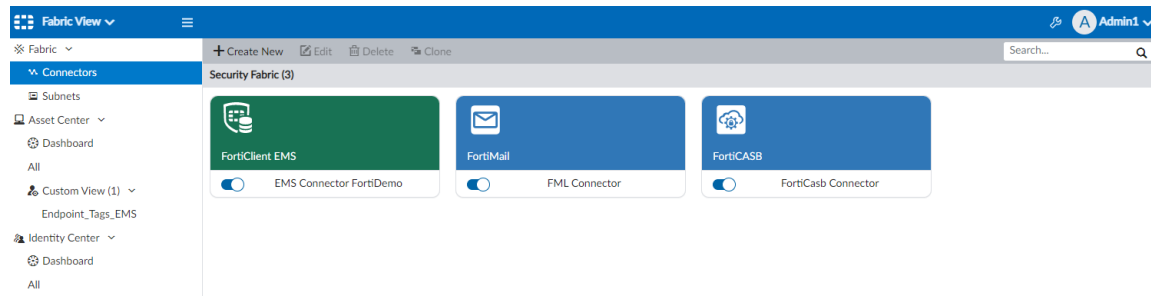
1. Go to *FortiSoC > Handlers > Event Handler List*.  
You can double-click the *Default-Shadow-IT-Events* event handler to view its filters.
2. Select the checkbox for *Default-Shadow-IT-Events*.
3. From the *More* dropdown, click *Enable*.

FortiSoC <span>Admin1</span>						
<div> <div> <div>+</div> <div>Create New</div> </div> <div> <div>✎</div> <div>Edit</div> </div> <div> <div>🗑</div> <div>Delete</div> </div> <div> <div>📄</div> <div>Clone</div> </div> <div> <div>⌵</div> <div>More</div> </div> </div>						
<input type="checkbox"/>	Status	Name	Filters	Devices	Send Alert to	Events
<input type="checkbox"/>	🟢	Default-FDC-Honey-Pot-Detection	> 1 Filter	All Devices		
<input type="checkbox"/>	🟢	Default-FCT-Threat-Detection-By-Thr	> 2 Filters	All Devices		20
<input type="checkbox"/>	🟢	Default-FCT-Threat-Detection-By-Enc	> 3 Filters	All Devices		20
<input type="checkbox"/>	🟢	Default-Recon-Activity-By-Endpoint	> 11 Filters	All Devices		71
<input type="checkbox"/>	🟢	Default-Compromised Host-Detection	> 3 Filters	All Devices		260
<input type="checkbox"/>	🟢	Default-Compromised Host-Detection	> 3 Filters	All Devices		96
<input type="checkbox"/>	🔴	Default-FFW System Events	> 8 Filters	All Devices		
<input type="checkbox"/>	🔴	Default-FFW-Compromised Host-Det	> 3 Filters	All Devices		
<input type="checkbox"/>	🔴	Default-FFW-Risky-Destination-Detection-By-Threat	> 10 Filters	All Devices		
<input type="checkbox"/>	🔴	Default-FFW-Risky-Destination-Detection-By-Endpoint	> 10 Filters	All Devices		
<input type="checkbox"/>	🔴	Default-FFW-Compromised Host-Detection-IOC-By-Endpoint	> 2 Filters	All Devices		
<input type="checkbox"/>	🔴	Default-FFW-Botnet-Communication-Detection-By-Endpoint	> 1 Filter	All Devices		
<input type="checkbox"/>	🔴	Default-FWB-Threat-Detection-By-Hostname	> 4 Filters	All Devices		
<input type="checkbox"/>	🔴	Default-FAI-Malware-Detection-By-FAI	> 1 Filter	All Devices		
<input type="checkbox"/>	🔴	Default-FSA-Malware-Handler-By-Threat	> 6 Filters	All Devices		
<input type="checkbox"/>	🔴	Default-FSA-Malware-Handler-By-Endpoint	> 4 Filters	All Devices		
<input type="checkbox"/>	🔴	Default-FSA-System-Handler	> 3 Filters	All Devices		
<input type="checkbox"/>	🔴	Default-FML-Threat-Detection-By-Email	> 11 Filters	All Devices		
<input checked="" type="checkbox"/>	🔴	Default-Shadow-IT-Events	> 3 Filters	All Devices		
<input type="checkbox"/>	🔴	Default-NOC-Interface-Events	> 4 Filters	All Devices		
<input type="checkbox"/>	🔴	Default-NOC-FortiExtender-Events	> 8 Filters	All Devices		
<input type="checkbox"/>	🔴	Default-NOC-Docker-Events	> 4 Filters	All Devices		
<input type="checkbox"/>	🔴	Local Device Event	> 1 Filter	Local Device		2

### To get cloud service data from the FortiCASB connector:

1. Go to *Fabric View > Connectors*.
2. Confirm there is an enabled *FortiCASB Connector*.

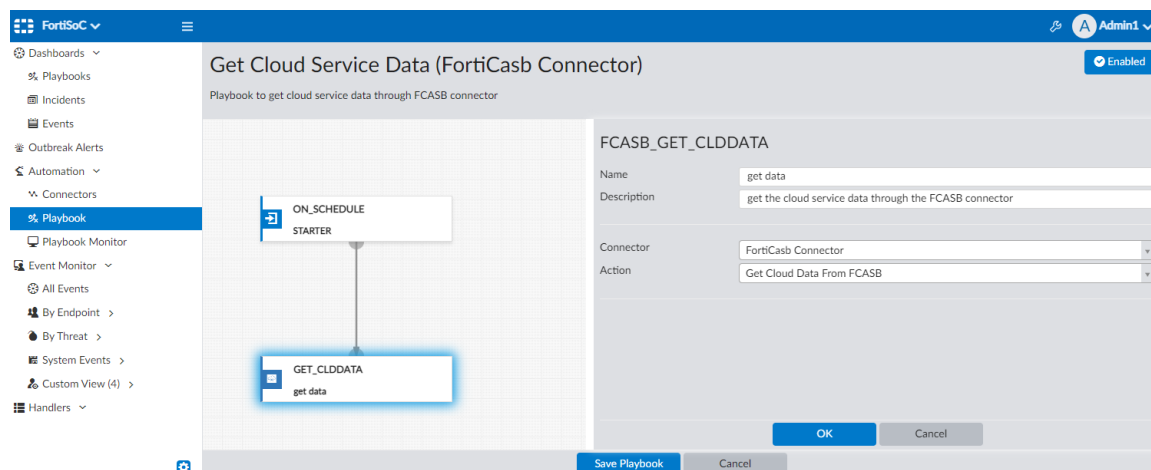
If there is not an enabled *FortiCASB Connector*, click *Create New* and choose *FortiCASB* under the *Security Fabric* category. Configure the FortiCASB connector settings, and click *OK*.



3. Go to *FortiSoC > Automation > Playbook*.
4. Confirm the *Get Cloud Service Data (FortiCasb Connector)* playbook is *Enabled*.  
This playbook is automatically created when you configure a FortiCASB connector in FortiAnalyzer.

Name	Description	Status	Created Time	Modified Time
Demo Playbook- Run Vuln Scan	Custom build playbook to get started	Enabled	02/11/2020	02/12/2020
Demo Playbook- Compromised Host I		Enabled	02/07/2020	08/25/2020
Demo Playbook- Critical Intrusion Inci		Enabled	02/07/2020	08/25/2020
Demo Playbook- Get Process List	Custom build playbook to get started	Enabled	02/11/2020	02/12/2020
Demo Playbook- Get Software Invento	Custom build playbook to get started	Enabled	02/11/2020	04/29/2020
Demo Playbook- Run AV Scan on dem	Custom build playbook to get started	Enabled	02/12/2020	02/12/2020
Demo Playbook- Update Assets and Id	Playbook to Update Asset and Identity	Enabled	01/30/2020	04/29/2020
Demo Playbook: Activate Strict IPS		Enabled	02/07/2020	04/21/2020
Demo Playbook: Add CnC IP to Blackli	Demo playbook to add CnC IP to Edge	Enabled	02/07/2020	02/12/2020
Demo Playbook: EMS Quarantine End		Enabled	02/07/2020	02/07/2020
Demo Playbook: EMS Unquarantine E	Demo playbook to unquarantine endp	Enabled	02/07/2020	02/12/2020
FOS Quarantine	Custom build playbook to get started	Enabled	04/15/2020	04/15/2020
<b>Get Cloud Service Data (FortiCasb Co</b>	<b>Playbook to get cloud service data thr</b>	<b>Enabled</b>	<b>05/03/2021</b>	<b>05/03/2021</b>
Get Software Inventory from EMS (EM	Playbook to get software inventory fr	Enabled	05/03/2021	05/03/2021
Get Vulnerabilities from EMS (EMS Co	Playbook to get vulnerabilities from E	Enabled	05/03/2021	05/03/2021
GetEndpointTagEMS	Custom build playbook to get started	Enabled	11/13/2020	11/13/2020
Update Asset and Identity Database (E	Playbook to automatically update Fort	Enabled	05/03/2021	05/03/2021

5. Double-click the *Get Cloud Service Data (FortiCasb Connector)* playbook to view its configuration.  
This playbook must get cloud service data through the FortiCASB connector for the *Default-Shadow-IT-Events* event handler to generate events.





## To view events generated by the shadow IT event handler:

1. Go to *FortiSoC > Event Monitor > All Events*.
2. Filter by Handler = Default-Shadow-IT-Events.

The screenshot shows the FortiSoC Event Monitor interface. The left sidebar contains navigation options: Dashboards, Playbooks, Incidents, Events, Outbreak Alerts, Automation, Connectors, Playbook, Playbook Monitor, Event Monitor, and All Events (selected). The main panel displays a table of events filtered by the handler 'Default-Shadow-IT-Events'. The table has columns for #, Event, Event Type, Additional Info, Handler, and Severity. The events listed are 'Unsanctioned Applications detected' and 'Unsanctioned Users detected', all with a severity of 'High' and handler 'Default-Shadow-IT-Events'.

#	Event	Event Type	Additional Info	Handler	Severity
1	Unsanctioned Applications detected	Application Control	Unsanctioned application YouTube with app risk: elevated detect...	Default-Shadow-IT-Events	High
	Unsanctioned Applications detected	Application Control	Unsanctioned application Facebook with app risk: medium detec...	Default-Shadow-IT-Events	High
	Unsanctioned Applications detected	Application Control	Unsanctioned application HTTP.BROWSER with app risk: media...	Default-Shadow-IT-Events	High
2	Unsanctioned Users detected	Application Control	Unsanctioned user: [] with app risk: elevated detected on: Branc...	Default-Shadow-IT-Events	High
3	Unsanctioned Applications detected	Application Control	Unsanctioned application YouTube with app risk: elevated detect...	Default-Shadow-IT-Events	High
	Unsanctioned Applications detected	Application Control	Unsanctioned application Facebook with app risk: medium detec...	Default-Shadow-IT-Events	High
	Unsanctioned Applications detected	Application Control	Unsanctioned application HTTP.BROWSER with app risk: media...	Default-Shadow-IT-Events	High
4	Unsanctioned Applications detected	Application Control	Unsanctioned application YouTube with app risk: elevated detect...	Default-Shadow-IT-Events	High
	Unsanctioned Applications detected	Application Control	Unsanctioned application Facebook with app risk: medium detec...	Default-Shadow-IT-Events	High
	Unsanctioned Applications detected	Application Control	Unsanctioned application HTTP.BROWSER with app risk: media...	Default-Shadow-IT-Events	High
5	Unsanctioned Applications detected	Application Control	Unsanctioned application YouTube with app risk: elevated detect...	Default-Shadow-IT-Events	High
	Unsanctioned Applications detected	Application Control	Unsanctioned application Facebook with app risk: medium detec...	Default-Shadow-IT-Events	High
	Unsanctioned Applications detected	Application Control	Unsanctioned application HTTP.BROWSER with app risk: media...	Default-Shadow-IT-Events	High
6	Unsanctioned Users detected	Application Control	Unsanctioned user: [] with app risk: elevated detected on: Branc...	Default-Shadow-IT-Events	High

## New event handlers for NOC monitoring

New default event handlers are added to detect FortiGate Interface events, FortiExtender events, and FortiManager MEA CPU and Memory related alerts.

There are three new predefined NOC event handlers available in the *Event Handler List*.

- Default-NOC-Docker-Events
- Default-NOC-FortiExtender-Events
- Default-NOC-Interface-Events

In addition, new filters are added to four existing predefined NOC event handlers:

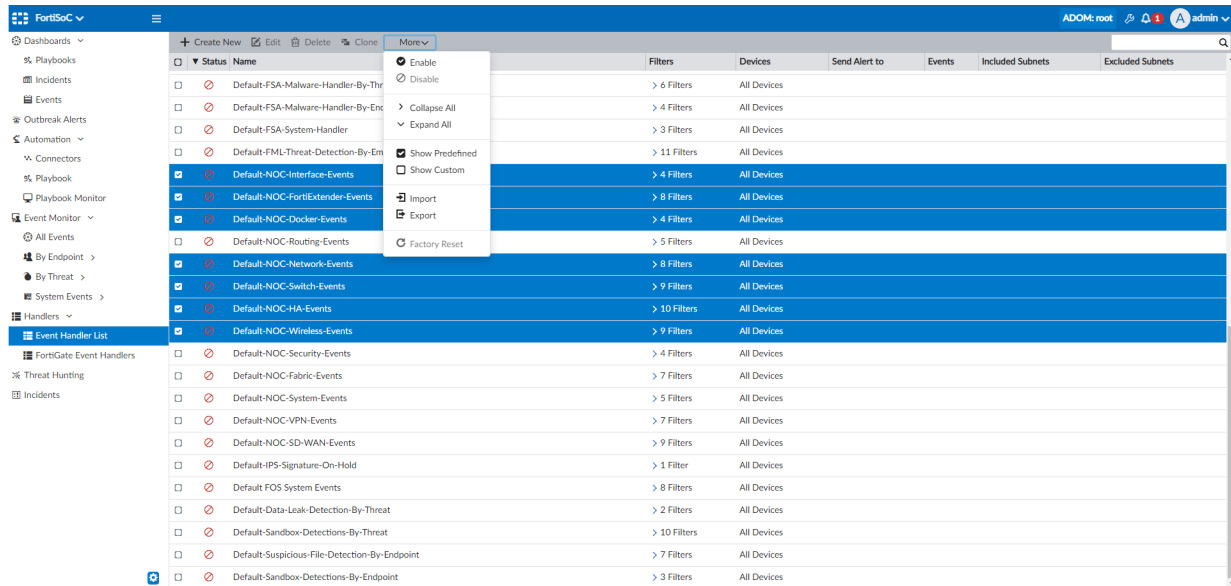
- Default-NOC-HA-Events
- Default-NOC-Network-Events
- Default-NOC-Switch-Events
- Default-NOC-Wireless-Events

All seven handlers are disabled by default and can be enabled according to need.

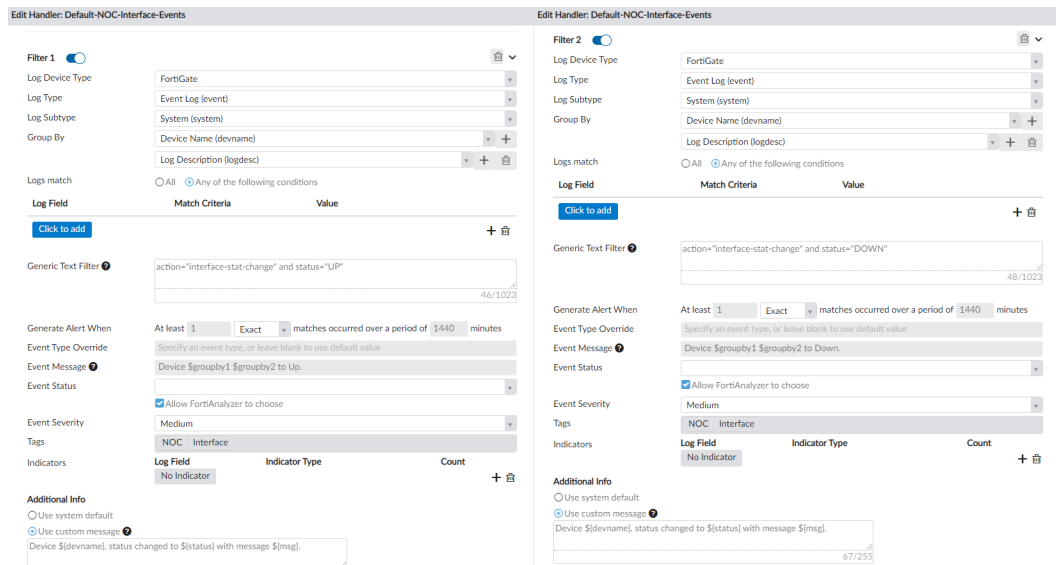
### To enable NOC event handlers:

1. Go to *FortiSoC > Handlers > Event Handler List*.
2. Select the checkbox for the NOC event handler(s) that you want to enable.

### 3. In the toolbar, click *More > Enable*.



You can double-click a NOC event handler to view its filters. For example, below are two predefined filters for the *Default-NOC-Interface-Events* event handler.



### To view events generated by enabled NOC event handlers:

1. Go to *FortiSoC > Event Monitor > All Events*.
2. Filter by *Handler* = a default NOC event handler. For example, *Handler* = *Default-NOC-Docker-Events*. Filtering by *Handler* = *Default-NOC-\*\*\** returns results for all enabled default NOC event handlers.

#	Event	Additional Info	Event Type	Count	Severity	Handler	Tags
1	FGV04TM21011436 [30]						
	Device FGV04TM21011436 DHCP server Object attribute configured	DHCP server status change ip-range: 1[-Delete-s...	System	4	Medium	Default-NOG:Network-Events	NOC   Network
	Device FGV04TM21011436 DHCP lease renewed. DHCP Ack log	Host medshetty-VM with message DHCP server...	System	4	Medium	Default-NOG:Network-Events	NOC   Network
	Device FGV04TM21011436 DNS Server Object attribute configured	Device FGV04TM21011436, DNS server statu...	System	1	Medium	Default-NOG:Interface-Events	NOC   Interface   DNS
	Device FGV04TM21011436 Interface status changed to Down.	Device FGV04TM21011436, status changed to...	System	2	Medium	Default-NOG:Interface-Events	NOC   Interface
	Device FGV04TM21011436 DNS Server Object configured	Device FGV04TM21011436, DNS server statu...	System	1	Medium	Default-NOG:Interface-Events	NOC   Interface   DNS
	Connection with CSF member established and authorized for device FGV04M...	Device FGV04TM21011436 Connected to Co...	System	1	Medium	Default-NOG:HA-Events	NOC   HA   Cluster
	FortiAnalyzer connection failed for FGV04TM21011436	Device FGV04TM21011436 Failed to connect ...	System	3	High	Default-NOG:HA-Events	NOC   HA   Cluster
	FortiAnalyzer connection up for FGV04TM21011436	Device FGV04TM21011436 Connected to For...	System	2	Medium	Default-NOG:HA-Events	NOC   HA   Cluster
	FortiManager tunnel connection down for device FGV04TM21011436	Device FGV04TM21011436 FortiManager tun...	System	1	High	Default-NOG:HA-Events	NOC   HA   Cluster
	FortiManager tunnel connection up for device FGV04TM21011436	Device FGV04TM21011436 FortiManager tun...	System	2	Medium	Default-NOG:HA-Events	NOC   HA   Cluster
	Device FGV04TM21011436 Interface status changed to Up.	Device FGV04TM21011436, status changed to...	System	1	Medium	Default-NOG:Interface-Events	NOC   Interface
	Device FGV04TM21011436 SNMP Attribute configured to Disable	Device FGV04TM21011436 Attribute configur...	System	1	Medium	Default-NOG:Network-Events	NOC   Network
	Device FGV04TM21011436 SNMP Attribute configured to Enable	Device FGV04TM21011436 Attribute configur...	System	1	Medium	Default-NOG:Network-Events	NOC   Network
	Signal-to-noise ratio on FGV04TM21011436 is poor	SSID log-test-sid..., has a poor quality SNR at [] d...	Wireless	200	Medium	Default-NOG:Wireless-Events	NOC   Wireless   Wifi   AP
	FGV04TM21011436 Rogue AP detected with SSID: log-test-sid	Rogue AP detected. SN: N/A with message: AP lo...	Wireless	1	Medium	Default-NOG:Wireless-Events	NOC   Wireless   Wifi   AP
	FGV04TM21011436 Fake AP detected with SSID: log-test-sid	Fake AP detected. SN: N/A	Wireless	1	Medium	Default-NOG:Wireless-Events	NOC   Wireless   Wifi   AP
	FGV04TM21011436 AP FAP22B0123456789 joined.	Physical AP join. of AP: FAP22B0123456789	Wireless	1	Medium	Default-NOG:Wireless-Events	NOC   Wireless   Wifi   AP
	FGV04TM21011436 AP FAP22B0123456789 left.	Physical AP leave. of AP: FAP22B0123456789	Wireless	1	Medium	Default-NOG:Wireless-Events	NOC   Wireless   Wifi   AP
	FGV04TM21011436 Failure happened on AP FAP22B0123456789.	Physical AP fail. of AP: FAP22B0123456789...	Wireless	30	Medium	Default-NOG:Wireless-Events	NOC   Wireless   Wifi   AP
	FGV04TM21011436 Wireless client associated	Wireless client associated for log-test-sid with m...	Wireless	1	Medium	Default-NOG:Wireless-Events	NOC   Wireless   Wifi   AP
	Signal-to-noise ratio on FGV04TM21011436 is fair	SSID log-test-sid..., has fair quality SNR at 25 dB	Wireless	45	Medium	Default-NOG:Wireless-Events	NOC   Wireless   Wifi   AP
	FGV04TM21011436 Wireless client authenticated	Wireless client authenticated for log-test-sid wit...	Wireless	1	Medium	Default-NOG:Wireless-Events	NOC   Wireless   Wifi   AP
	FGV04TM21011436 Wireless client disassociated	Wireless client disassociated for log-test-sid wit...	Wireless	1	Medium	Default-NOG:Wireless-Events	NOC   Wireless   Wifi   AP
	FGV04TM21011436 Wireless client deauthenticated	Wireless client deauthenticated for log-test-sid ...	Wireless	1	Medium	Default-NOG:Wireless-Events	NOC   Wireless   Wifi   AP
	FGV04TM21011436 Wireless client idle	Wireless client idle for log-test-sid with message...	Wireless	1	Medium	Default-NOG:Wireless-Events	NOC   Wireless   Wifi   AP

## Include IOC detected on FortiGate local traffic in FortiAnalyzer IOC view

FortiGate devices generate an event log for indicators of compromise (IOC) when they are detected in local out traffic. FortiAnalyzer displays this data in *FortiView* > *FortiView* > *Threats* > *Compromised Hosts*.

To view IOC detected on FortiGate local traffic:

1. Go to *FortiView* > *FortiView* > *Threats* > *Compromised Hosts*.

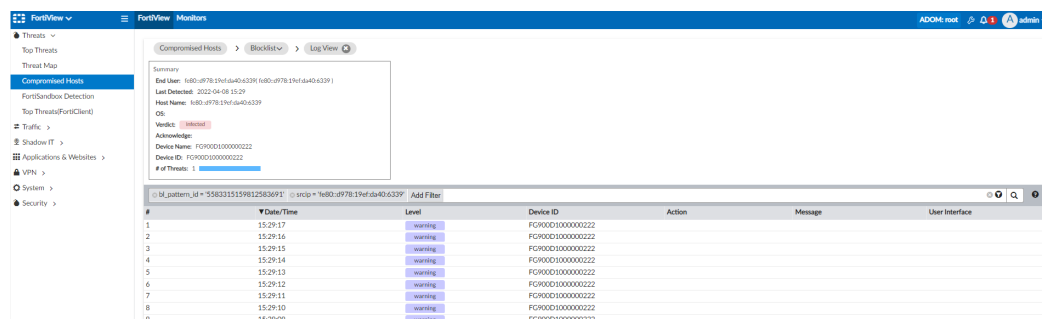
#	End User	Last Detected	Host Name	OS	Threat	# of Threats	Acknowledge	Device Name	Device ID
1	1680-9778-17ef-da0-6339	2022-04-08 15:28	1680-9778-17ef...	Windows	Infected	1	Yes	FGV0001000000222	FGV0001000000222
2	172.17.81.37	2022-04-08 14:14	172.17.81.37	Windows	Infected	3	Yes	FGV0001000000222	FGV0001000000222
3	10.2.60.111	2022-04-08 13:53	10.2.60.111	Windows	Infected	1	Yes	FGV0001000000222	FGV0001000000222
4	172.16.65.221	2022-04-07 23:29	VAN-201692-PC	Windows	High Suspicious	1	Yes	FGV0001000000222	FGV0001000000222
5	172.16.62.14	2022-04-07 22:59	172.16.62.14	Windows	High Suspicious	1	Yes	FGV0001000000222	FGV0001000000222
6	172.16.65.120	2022-04-07 22:59	172.16.65.120	Windows	High Suspicious	1	Yes	FGV0001000000222	FGV0001000000222
7	110.110.110.112	2022-04-07 21:59	110.110.110.112	Windows	High Suspicious	1	Yes	FGV0001000000222	FGV0001000000222
8	110.110.110.110	2022-04-07 21:59	110.110.110.110	Windows	High Suspicious	1	Yes	FGV0001000000222	FGV0001000000222

2. Double-click the row for a compromised host.

The *Threat Name* = *botnet* and the *Detect Pattern*= the destination IP.

#	Detect Pattern	Threat Type	Threat Name	Category	Detect Method	# of Events	Log Type	Security Actions	Scan Time
1	1680-16	Threat Type	botnet	Category	detected by fgt	120	event	Details	2022-04-08 15:29:48

3. Double-click the row for the detect pattern.  
You can review the related logs for the IOC.

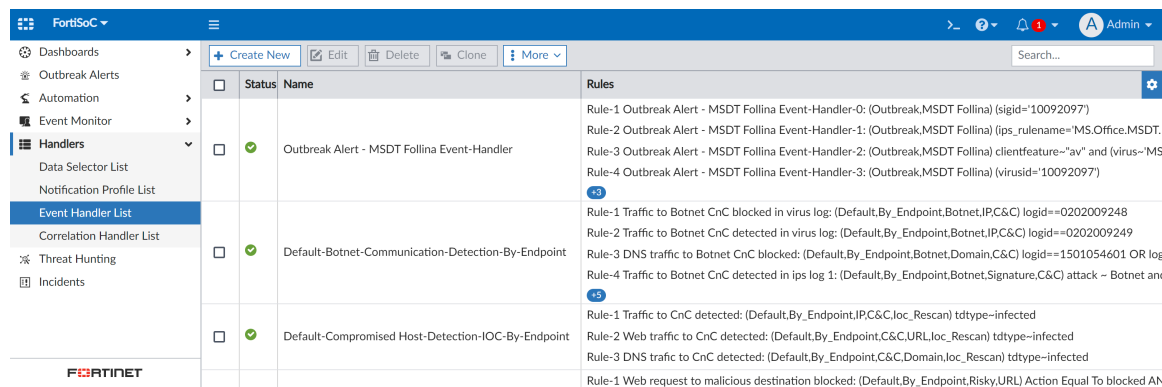


## Rule based event correlation - 7.2.2

In previous versions, event handlers could only be triggered when individual filters were matched. Rule based event correlation gives extra flexibility by triggering event handlers when a *series* of rules are met.

Usability is also enhanced with the introduction of data selectors and notification profiles. You can define devices, log filters, and notification parameters that can be used across multiple event handlers without the need to re-create them individually in each event handler.

These features are configured in *FortiSoC > Handlers*. This pane now includes a *Data Selector List*, *Notification Profile List*, *Event Handler List*, and *Correlation Handler List*.



The following is available in this topic:

- [Data selectors](#)
- [Notification profiles](#)
- [Event handlers](#)
- [Correlation handlers](#)

### Data selectors

Data selectors are used to select devices, subnets, and filters (previously known as "pre-filters") for event handlers. You can create, edit, clone, and delete data selectors in *FortiSoC > Handlers > Data Selector List*.

There are five default data selectors:

- *Default Intrusion Selector For Malicious Code Detection*
- *Default IP Scanning Selector For Recon Activity Detection*
- *Default Local Device Selector*

- *Default Malicious File Selector For Malicious File Detection*
- *Default Risky App Selector for Risky App Detection*

These default data selectors are used in some of the predefined event handlers, and they cannot be edited or deleted.

Name	Devices	Rules
Default Intrusion Selector For Malicious Code Detection	All Devices	Rule-1 Intrusion: attack!~Botnet and logid~041901638[4-6]
Default IP Scanning Selector For Recon Activity Detection	All Devices	Rule-1 IP_scanning: (action~"client-rst timeout deny") and srcintfrole!=wan and dstintfrole!=wan
Default Local Device Selector	Local Devices	
Default Malicious File Selector For Malicious File Detection	All Devices	Rule-1 Malicious_File: logid~021100819[2-5]
Default Risky App Selector For Risky App Detection	All Devices	Rule-1 Risky_App: apprisk~"critical high"

When configuring a data selector, you must specify:

- Devices
- Subnets
- Filters



The filters in data selectors are applied before every rule configured in the event handler. As a result, the filters do not need to be configured individually within each rule of the event handler (s) that the data selector is assigned to.

**Add New Data Selector**

Name: TestSelector

Devices: All Devices | Specify | Local Device

Subnets: All Subnets | Specify

Include Subnets: lab (1 entry selected)

Exclude Subnets: qanetwork (1 entry selected)

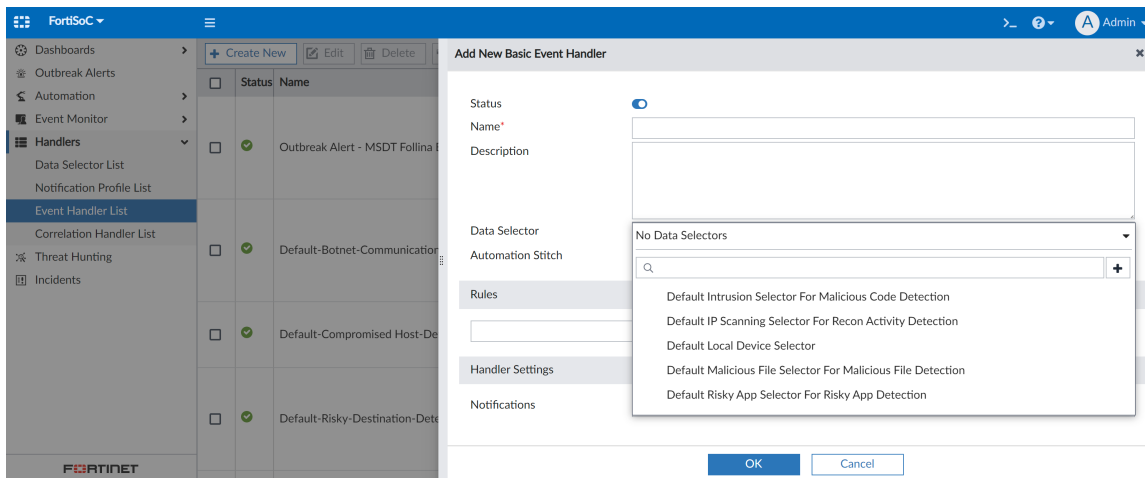
Filters: Any of the following conditions

FortiGate-Traffic

FortiClient-Event

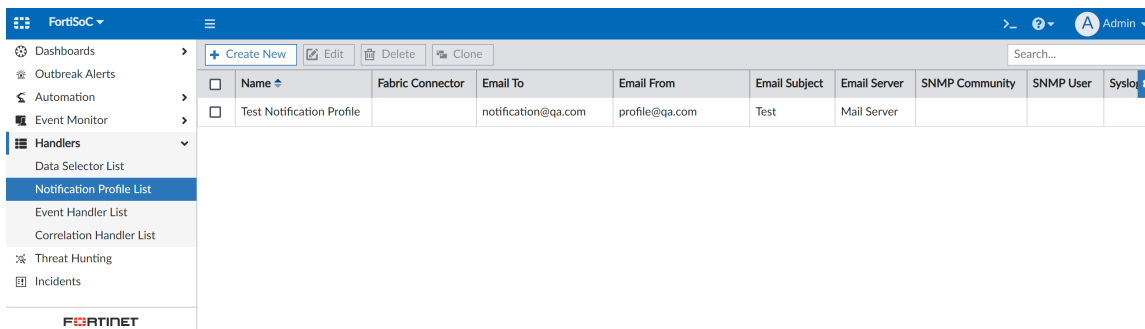
OK Cancel

Once configured, the data selectors can be applied to basic event handlers and correlation event handlers, where needed.

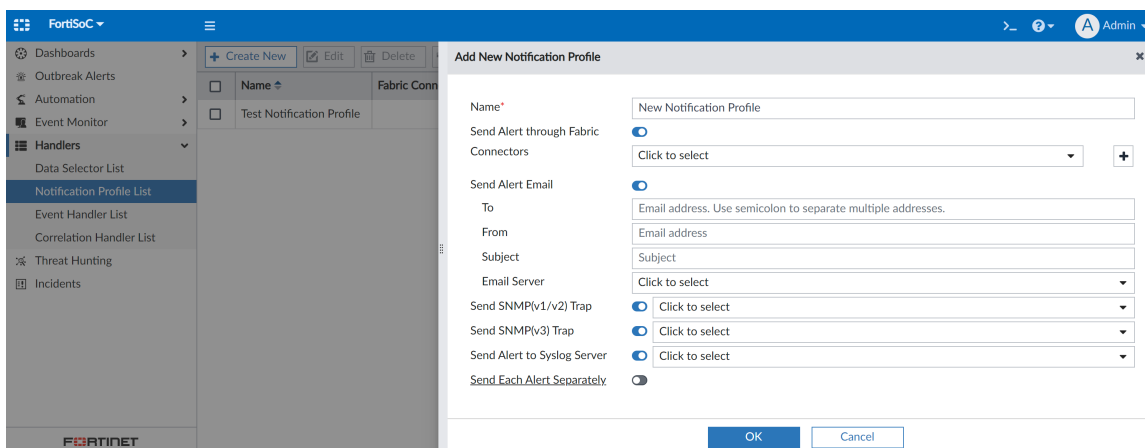


## Notification profiles

Notification profiles determine if and where an event handler sends an alert notification when generating an event. You can create, edit, clone, and delete notification profiles in *FortiSoC > Handlers > Notification Profile List*.



You can configure the notification profile to send the alert to an email address, SNMP community, and/or syslog server. You can also configure the notification profile to send the alert through a fabric connector.



Similar to data selectors, notification profiles can be assigned to basic event handlers and correlation event handlers, where needed.

## Event handlers

You can create, edit, clone, delete, and import/export basic event handlers in *FortiSoC > Handlers > Event Handler List*.

When creating and editing an event handler, you can assign a data selector and notification profile.

You can also configure the event handler rules according to your needs.

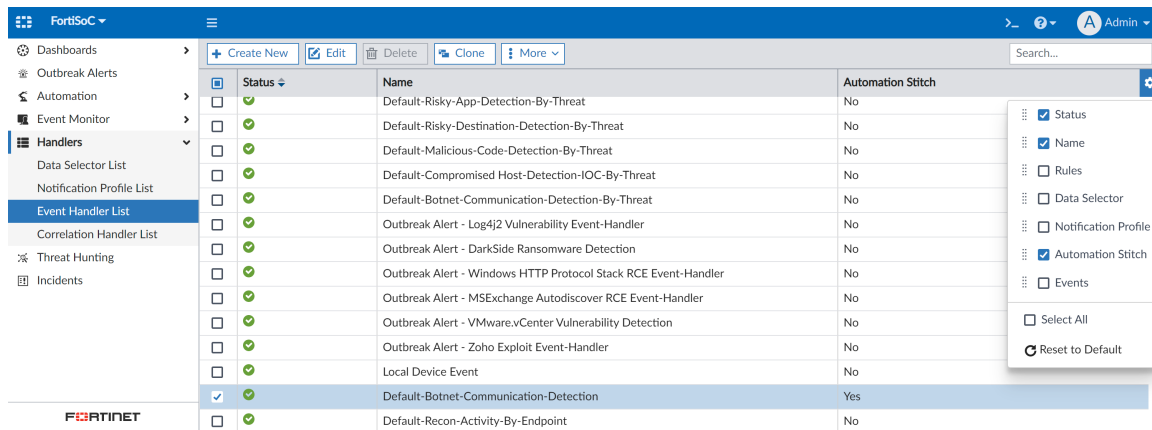


The event handler "rules" were previously known as "filters".

The *Automation Stitch* option is now available when configuring event handlers. Events triggered from event handlers with the automation stitch enabled are pushed to the FortiGate for further processing. These events can be viewed in the FortiAnalyzer GUI as well. For example, see the predefined event handler below with *Automation Stitch* enabled.

An *Automation Stitch* column is added in the *Event Handler List* to identify which event handlers have the automation stitch enabled.





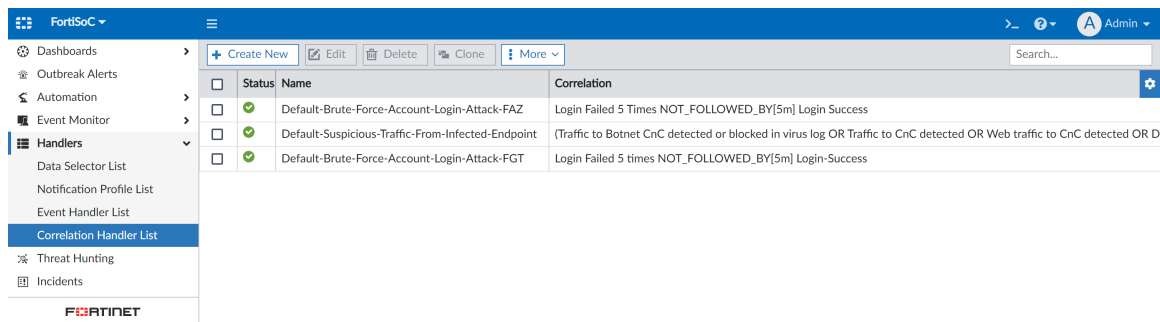
## Correlation handlers

You can create, edit, clone, delete, and import/export correlation event handlers in *FortiSoC > Handlers > Correlation Handler List*.

There are three default correlation handlers:

- *Default-Brute-Force-Account-Login-Attack-FAZ*
- *Default-Brute-Force-Account-Login-Attack-FGT*
- *Default-Suspicious-Traffic-From-Infected-Endpoint*

These correlation handlers are disabled by default. Some of their settings can be edited, and they can be enabled according to your needs. To enable the correlation handlers, as they are in the image below, select the correlation handler and click *More > Enable*.



Similar to basic event handlers, you can assign a data selector and notification profile to the correlation event handler. You can also enable the *Automation Stitch*, if needed.

When configuring rules for the correlation event handler, you must also configure a correlation sequence and correlation criteria for those rules. For example, see the default correlation handler below.

**Edit Correlation Event Handler**

Status: ☒

Name: Default-Brute-Force-Account-Login-Attack-FAZ

Description: This handler is to detect if an account login failed many times not followed by a login success for FortiAnalyzer.

Automation Stitch: ☒

Data Selector: Click to select

Threshold Duration: 30

**Correlation Sequence**

- + New Correlation Group
  - Login Failed 5 Times (NOT\_FOLLOWED\_BY 5m)
    - Login Success

Show Raw Config: ☒

**Correlation Criteria**

Rule	Field	Match Criteria	Rule	Field	Action
Login Failed 5 Times	devid	=	Login Success	devid	

**Handler Settings**

Event Type Override: Specify an event type, or leave blank to use default value

Event Message: Click to select

Event Status: ☒ Allow FortiAnalyzer to choose

Event Severity: Medium

OK Cancel

When creating a new correlation handler, you can add rules using the plus (+) icon in the *Correlation Sequence* section.

**Add New Correlation Event Handler**

Status: ☒

Name:

Description:

Automation Stitch: ☒

Data Selector: Click to select

Threshold Duration: 30

**Correlation Sequence**

- + New Correlation Group
  - Login Failed 5 Times (NOT\_FOLLOWED\_BY 5m)
    - Login Success

Show Raw Config: ☒

**Correlation Criteria**

Rule	Field	Match Criteria	Rule	Field	Action
Login Failed 5 Times	devid	=	Login Success	devid	

**Handler Settings**

Event Type Override: Specify an event type, or leave blank to use default value

Event Message: Click to select

Event Status: ☒ Allow FortiAnalyzer to choose

Event Severity: Medium

OK Cancel

You can configure the same options in a rule for a correlation handler as in a basic event handler. For example, see a rule from the default correlation handler below.

**Add New Rule**

Name:

Log Device Type: FortiGate

Log Type: Event Log (event)

Log Subtype: Any (\_any\_)

Group By: CSF Name (csfname)

Logs match: All

Log Field	Match Criteria	Value	Action
+			

Generic Text Filter:

Aggregation Expression: COUNT >= 1

OK Cancel

Rules are added to the correlation sequence in the order that they are created. You can create the rules in the desired order for the sequence, or re-order them into the correlation sequence after they are created. After creating the rules, use the dropdown to select other rules created in the correlation handler, thereby changing the sequence order.

**Edit Correlation Event Handler**

Status: ☒

Name: Default-Brute-Force-Account-Login-Attack-FAZ

Description: This handler is to detect if an account login failed many times not followed by a login success for FortiAnalyzer.

Automation Stitch: ☐

Data Selector: Click to select

Threshold Duration: 30

**Correlation Sequence**

+ New Correlation Group

- Login Failed 5 Times
  - LOWED\_BY: 5m
  - Login Success

Correlation Criteria

Rule	Field	Match Criteria	Rule	Field	Action
Login Failed 5 Times	devid	=	Login Success	devid	x +

Handler Settings

OK Cancel

All rules must be met in correlation sequence to generate an event. You can select from the following options to set the relationship between each rule in sequence:

- AND
- AND\_NOT
- OR
- FOLLOWED\_BY (if selected, enter a time limit for the correlation to occur in)
- NOT\_FOLLOWED\_BY (if selected, enter a time limit for the correlation to occur in)

**Edit Correlation Event Handler**

Status: ☒

Name\*: Default-Brute-Force-Account-Login-Attack-FAZ

Description: This handler is to detect if an account login failed many times not followed by a login success for FortiAnalyzer.

Automation Stitch: ☒

Data Selector: Click to select

Threshold Duration: 30

**Correlation Sequence**

+ New Correlation Group

Login Failed 5 Times NOT\_FOLLOWED\_BY 5m

Login Success

Show Raw Config: ☒

**Correlation Criteria**

Rule	Field	Rule	Field	Action
Login Failed 5 Times	devid	Login Success	devid	x +

Handler Settings

OK Cancel

You can edit or delete rules within the correlation sequence by using the icons next to the rule. Alternatively, you can click the edit icon in the rule dropdown to edit its settings.

**Edit Correlation Event Handler**

Status: ☒

Name\*: Default-Brute-Force-Account-Login-Attack-FAZ

Description: This handler is to detect if an account login failed many times not followed by a login success for FortiAnalyzer.

Automation Stitch: ☒

Data Selector: Click to select

Threshold Duration: 30

**Correlation Sequence**

+ New Correlation Group

Login Failed 5 Times FOLLOWED\_BY 5m

Login Success

Show Raw Config: ☒

**Correlation Criteria**

Rule	Field	Match Criteria	Rule	Field	Action
Login Failed 5 Times	devid	=	Login Success	devid	x +

Handler Settings

OK Cancel

In the *Correlation Criteria* section, you can specify the fields that the event handler will look for to correlate the rules. You can add multiple correlation criteria, if needed. Each correlation criteria is applied to two rules, using a field from each rule to correlate the two. The options available in the *Field* dropdown are determined by the *Group By* fields configured in the rules. For example, see the correlation criteria from the default correlation handler.

The image displays two screenshots of the FortiSoC 'Edit Correlation Event Handler' configuration page. The top screenshot shows the 'Correlation Criteria' section with a dropdown menu open for 'Login Failed 5 Times'. The bottom screenshot shows the 'Handler Settings' section with a dropdown menu open for 'devid'.

Events generated from both basic event handlers and correlation event handlers appear in *FortiSoC > Event Monitor*.

## Data exfiltration detection - 7.2.2

The aggregation expression *SUM* has been introduced to calculate log field values within a certain period. Event handlers can use the *SUM* expression to trigger events/notifications when the content of log fields reach a certain threshold.

This new feature is used to detect data exfiltration attempts.

The *Aggregation Expression* can be set to *SUM* when configuring rules for both event handlers and correlation handlers. For more information about correlation handlers, see [Rule based event correlation 7.2.2 on page 28](#).

### To use the *SUM* aggregation expression in an event handler:

1. Go to *FortiSoC > Handlers > Event Handler List*, and click *Create New*.
2. Click *Add New Rule*.

You can also edit or clone an event handler to edit an existing rule.

3. From the *Aggregation Expression* dropdown, select *SUM*.

The screenshot shows the 'Add New Rule' configuration window in FortiSoC. The left sidebar contains navigation options like Dashboards, Outbreak Alerts, Automation, Event Monitor, Handlers, Data Selector List, Notification Profile List, Event Handler List, Correlation Handler List, Threat Hunting, and Incidents. The main configuration area includes fields for Status, Name, Log Device Type (FortiGate), Log Type (Traffic Log (traffic)), Log Subtype (Any), Group By (Application Name (app)), and Logs match (All). A dropdown menu for 'Any of the following conditions' is open, showing 'COUNT', 'COUNT\_DISTINCT', and 'SUM' (selected). Below this, a table with columns 'Log Field', 'Match Criteria', 'Value', and 'Action' is visible. The first row shows 'Level (pri)' with 'Equal To' criteria and 'Emergency' value. At the bottom, the 'Aggregation Expression' is set to 'SUM' and the 'Value' field is '1'.

4. Enter the following for the *Aggregation Expression*:

Option	Description
<b>Aggregation field</b>	Select an aggregation field from the dropdown. The available options depend on the <i>Log Device Type</i> and <i>Log Type</i> selected for the rule.
<b>Threshold</b>	Enter the threshold value required to satisfy the rule. When the data from multiple logs reaches this sum threshold, the rule condition will be satisfied.
<b>Multiplier</b>	For some aggregation fields, you can select a multiplier for the threshold value. For example, when <i>sentbyte</i> is selected as the aggregation field, you can select one of the following multipliers: <ul style="list-style-type: none"> <li>• <i>null</i> (bytes)</li> <li>• <i>Kilo Byte</i></li> <li>• <i>Mega Byte</i></li> <li>• <i>Giga Byte</i></li> <li>• <i>Terra Byte</i></li> </ul>

5. In the *Aggregation Duration* field, enter the number of minutes the logs have to reach this sum in order to satisfy the rule.
6. Configure the remaining options for the rule and the event handler, as needed.

### Example:

Below is an event handler configured to generate an alert when a total of 100MB of data is sent from an endpoint within 30 minutes:

- *Aggregation Expression = SUM*

<b>Aggregation field</b>	sentbyte
<b>Threshold</b>	100
<b>Multiplier</b>	Mega Byte

- *Aggregation Duration = 30*

**Edit Rule**

Status: ☒

Name: sentbyte-greater-than-or-equal-to-100MB

Log Device Type: FortiGate

Log Type: Traffic Log (traffic)

Log Subtype: Any

Group By: Source Endpoint (endpoint)

Logs match: All **Any of the following conditions**

Log Field	Match Criteria	Value	Action
+			

Generic Text Filter

Aggregation Expression: SUM sentbyte >= 100 Mega Byte

Aggregation Duration: 30

OK Cancel

Events triggered by this event handler appear in *FortiSoC > Event Monitor > All Events*. For example, see the image below.

#	Event	Event Type	Count	Severity	First Occurrence	Handler
1	> 10.2.129.60 (2)	Traffic	47	Medium	An hour ago	SUM-Handler
2	> 192.168.174.219 (2)	Traffic	379	Medium	An hour ago	SUM-Handler
3	> 192.168.174.217 (2)	Traffic	352	Medium	An hour ago	SUM-Handler
4	> 192.168.174.45 (2)	Traffic	224	Medium	An hour ago	SUM-Handler
5	> 10.2.107.41 (2)	Traffic	70	Medium	An hour ago	SUM-Handler
6	> 192.168.50.20 (2)	Traffic	9297	Medium	An hour ago	SUM-Handler
7	> 10.2.0.250 (1)	Traffic	1042	Medium	An hour ago	SUM-Handler

## Dashboards

This section lists the new features added to FortiAnalyzer for dashboards:

- SD-WAN chart to include more ADVPN shortcut information on page 40
- SD-WAN chart for MOS scoring on page 42
- Add ZTNA dashboard to FortiView on page 46
- IoT visibility on page 49
- Traffic shaping charts 7.2.1 on page 50

- [CASB Apps Access widget 7.2.1 on page 53](#)
- [Auto-refresh on FortiSoC dashboard elements 7.2.2 on page 54](#)

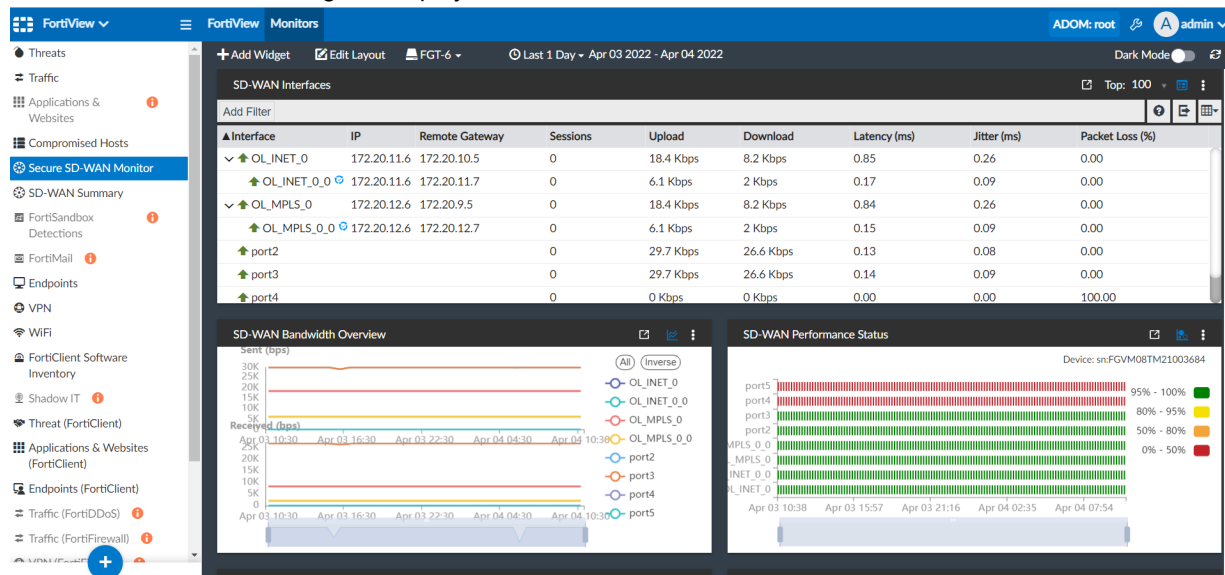
## SD-WAN chart to include more ADVPN shortcut information

The *SD-WAN Interfaces* widget is available in *FortiView > Monitors > Secure SD-WAN Monitor*.

This widget displays the following information for SD-WAN interfaces: IP, Remote Gateway, Sessions, Upload, Download, Latency (ms), Jitter (ms), and Packet Loss (%). The Upload and Download columns can be used to show outbound and inbound bandwidth. For a VPN tunnel interface, IP and Remote Gateway are the local IP and Remote Gateway IP of the VPN tunnel.

### To view the SD-WAN interface information:

1. Go to *FortiView > Monitors > Secure SD-WAN Monitor*.  
The SD-WAN Interfaces widget is displayed.



2. If there is an expand icon in the row, click the icon to view the ADVPN shortcut information in a row below. The IP and Remote Gateway are the local spoke IP and remote spoke IP of the shortcut VPN tunnel.



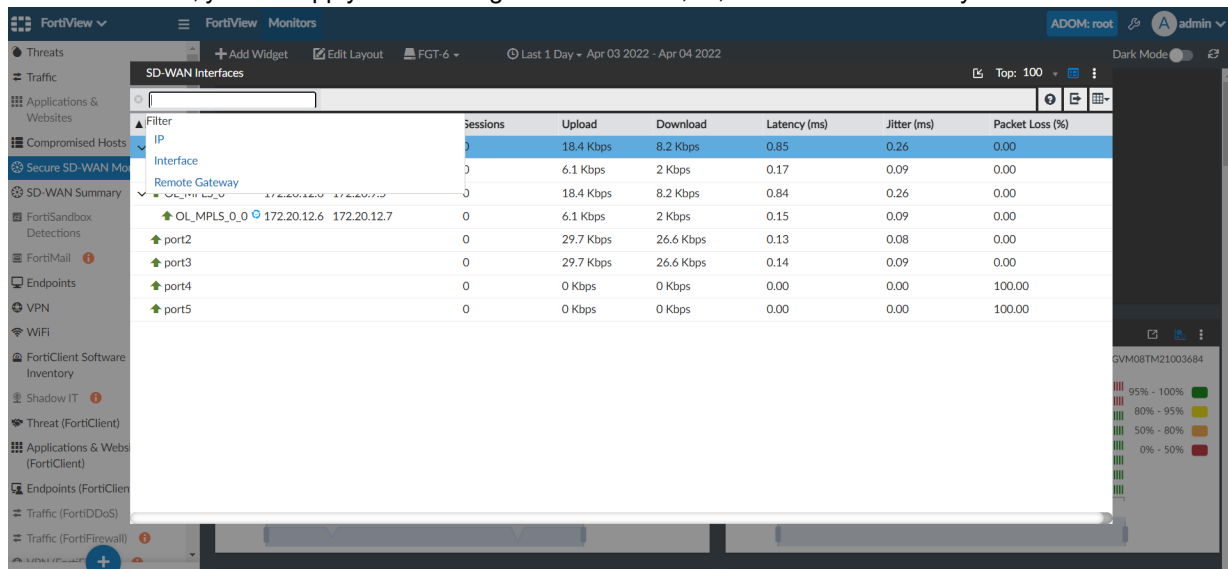
The screenshot shows the FortiView interface with the 'SD-WAN Interfaces' widget selected. The widget displays a table with the following data:

Interface	IP	Remote Gateway	Sessions	Upload	Download	Latency (ms)	Jitter (ms)	Packet Loss (%)
OL_INET_0	172.20.11.6	172.20.10.5	0	18.4 Kbps	8.2 Kbps	0.85	0.26	0.00
OL_INET_0_0	172.20.11.6	172.20.11.7	0	6.1 Kbps	2 Kbps	0.17	0.09	0.00
OL_MPLS_0	172.20.12.6	172.20.9.5	0	18.4 Kbps	8.2 Kbps	0.84	0.26	0.00
OL_MPLS_0_0	172.20.12.6	172.20.12.7	0	6.1 Kbps	2 Kbps	0.15	0.09	0.00
port2			0	29.7 Kbps	26.6 Kbps	0.13	0.08	0.00
port3			0	29.7 Kbps	26.6 Kbps	0.14	0.09	0.00
port4			0	0 Kbps	0 Kbps	0.00	0.00	100.00
port5			0	0 Kbps	0 Kbps	0.00	0.00	100.00

The following information is available in the widget:

<b>Interface</b>	The name of the interface.
<b>IP</b>	The IP address for the interface.
<b>Remote Gateway</b>	The remote gateway IP address.
<b>Sessions</b>	The number of sessions for the interface.
<b>Upload</b>	The upload speed for the interface.
<b>Download</b>	The download speed for the interface.
<b>Latency (ms)</b>	The latency for the interface.
<b>Jitter (ms)</b>	The jitter for the interface.
<b>Packet Loss (%)</b>	The packet loss for the interface.

3. In the table chart, you can apply the following filters: Interface, IP, and Remote Gateway.



Filter	Sessions	Upload	Download	Latency (ms)	Jitter (ms)	Packet Loss (%)
IP	0	18.4 Kbps	8.2 Kbps	0.85	0.26	0.00
Interface	0	6.1 Kbps	2 Kbps	0.17	0.09	0.00
Remote Gateway	0	18.4 Kbps	8.2 Kbps	0.84	0.26	0.00
OL_MPLS_0_0 172.20.12.6 172.20.12.7	0	6.1 Kbps	2 Kbps	0.15	0.09	0.00
port2	0	29.7 Kbps	26.6 Kbps	0.13	0.08	0.00
port3	0	29.7 Kbps	26.6 Kbps	0.14	0.09	0.00
port4	0	0 Kbps	0 Kbps	0.00	0.00	100.00
port5	0	0 Kbps	0 Kbps	0.00	0.00	100.00

## SD-WAN chart for MOS scoring

An *Audio MOS Score* widget is added to *FortiView > Monitors > Secure SD-WAN Monitor* and *FortiView > Monitors > SD-WAN Summary*. These widgets display logs for the MOS (mean opinion score) of voice and video traffic.

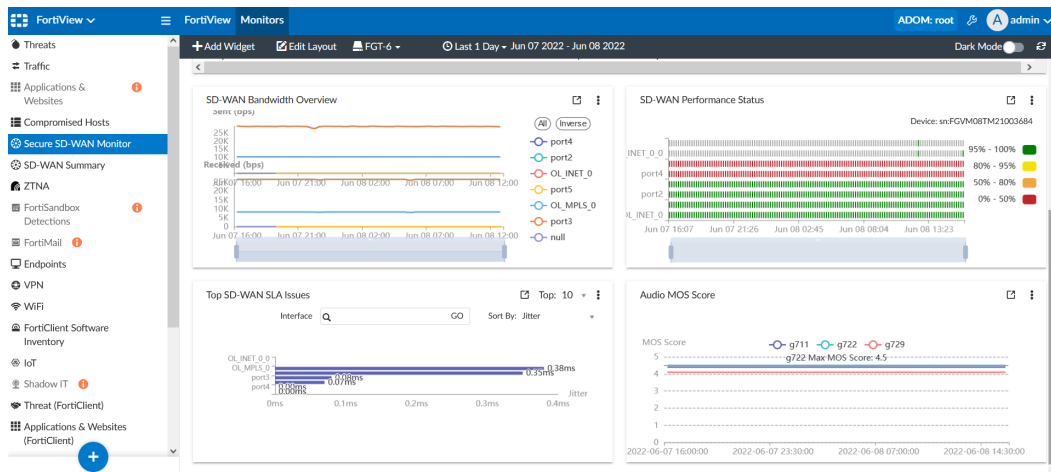
MOS is a method to measure the impact network quality has on the quality of a voice call. It is the industry standard for measuring voice and video quality on a WAN link.



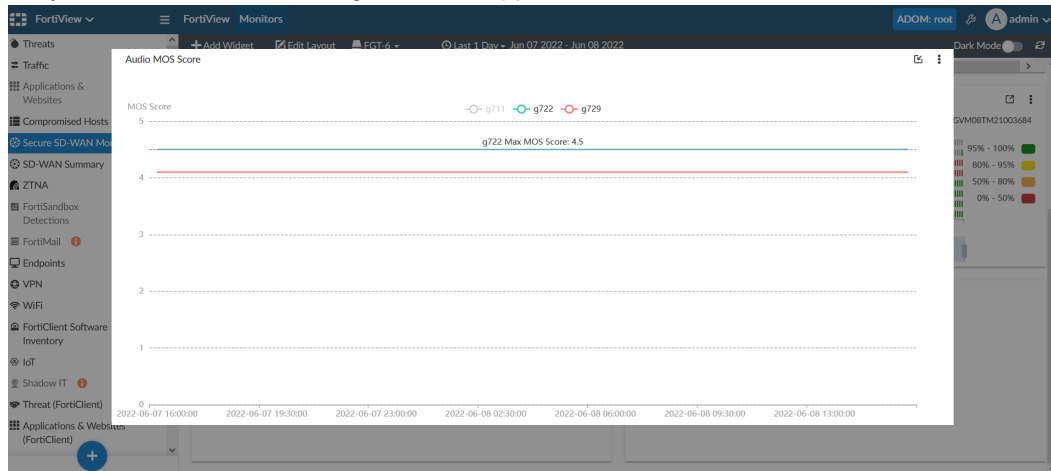
The FortiGate version must be on version 7.2 or later and have the MOS codec and MOS threshold attributes defined for SD-wan health check in order for FortiAnalyzer to display information in the MOS scoring widgets.

### To view the Audio MOS Score for individual devices:

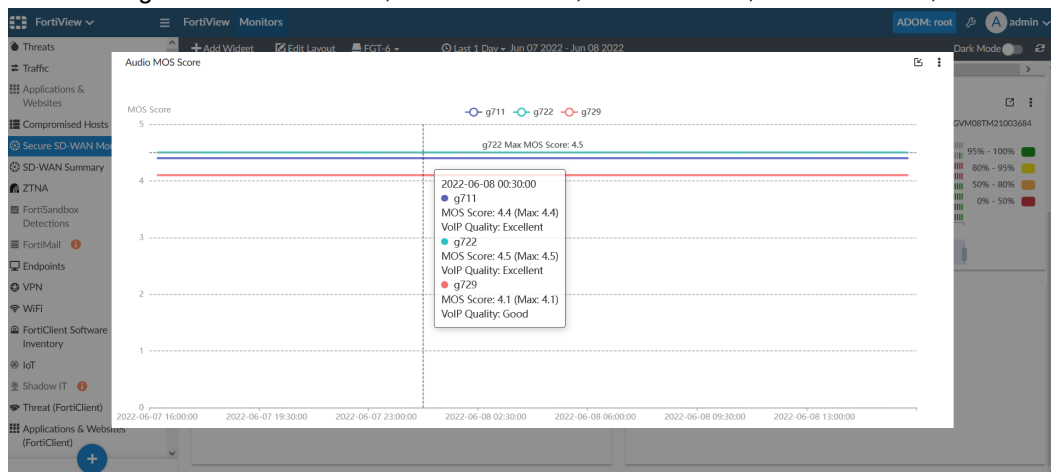
1. Go to *FortiView > Monitors > Secure SD-WAN Monitor*.
2. Click *Add Widget*, and add the *Audio MOS Score* widget.  
The widget includes a line graph of the MOS score for different codecs for the selected device over a specified time period.



- Click a codec in the legend to make it appear/disappear on the chart.  
Greyed-out interfaces on the legend do not appear on the chart.



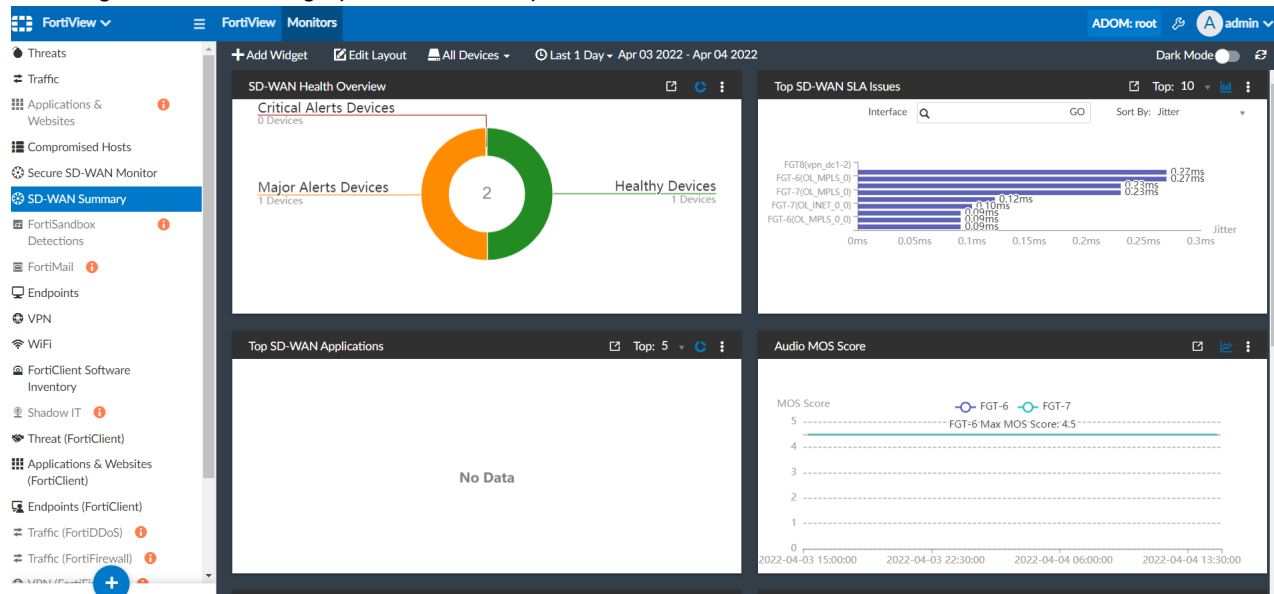
- Hover your cursor over the chart to see a summary at that point.  
This summary includes the MOS score and the VoIP quality at that time. VoIP quality is divided into levels based on MOS scoring: Excellent = 4.3 - 5.0, Good = 4.0 - 4.3, Fair = 3.6 - 4.0, Poor = 3.1 - 3.6, Bad = 2.6 - 3.1.



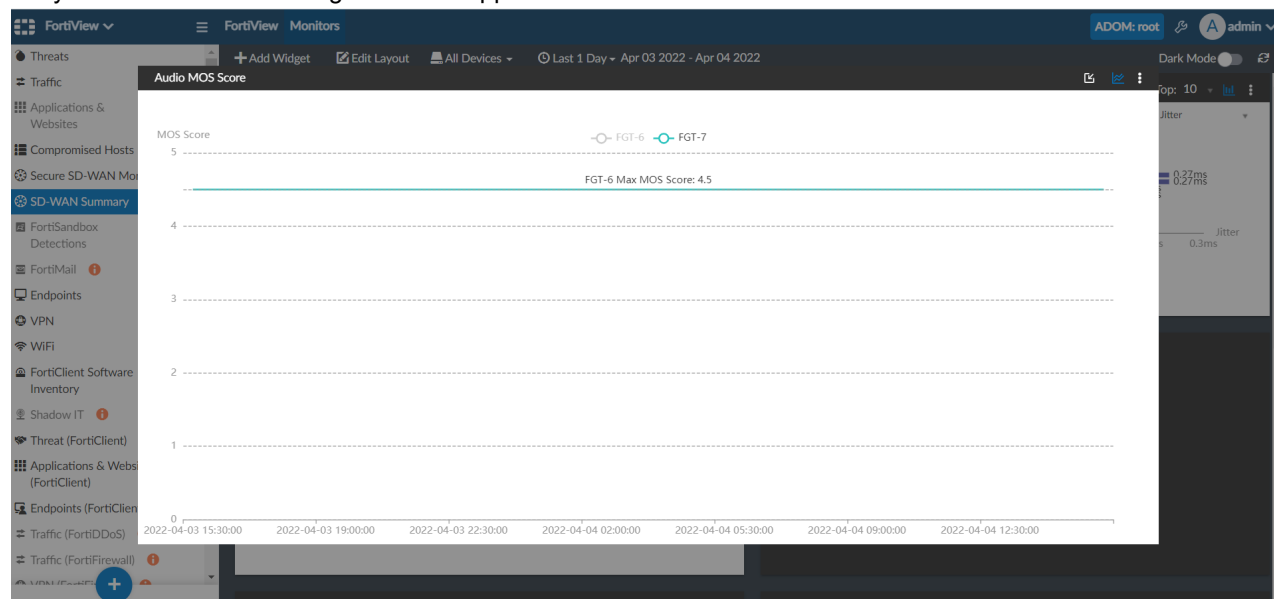
### To view the Audio MOS Score across all devices:

1. Go to *FortiView > Monitors > SD-WAN Summary*.
2. Click *Add Widget*, and add the *Audio MOS Score* widget.

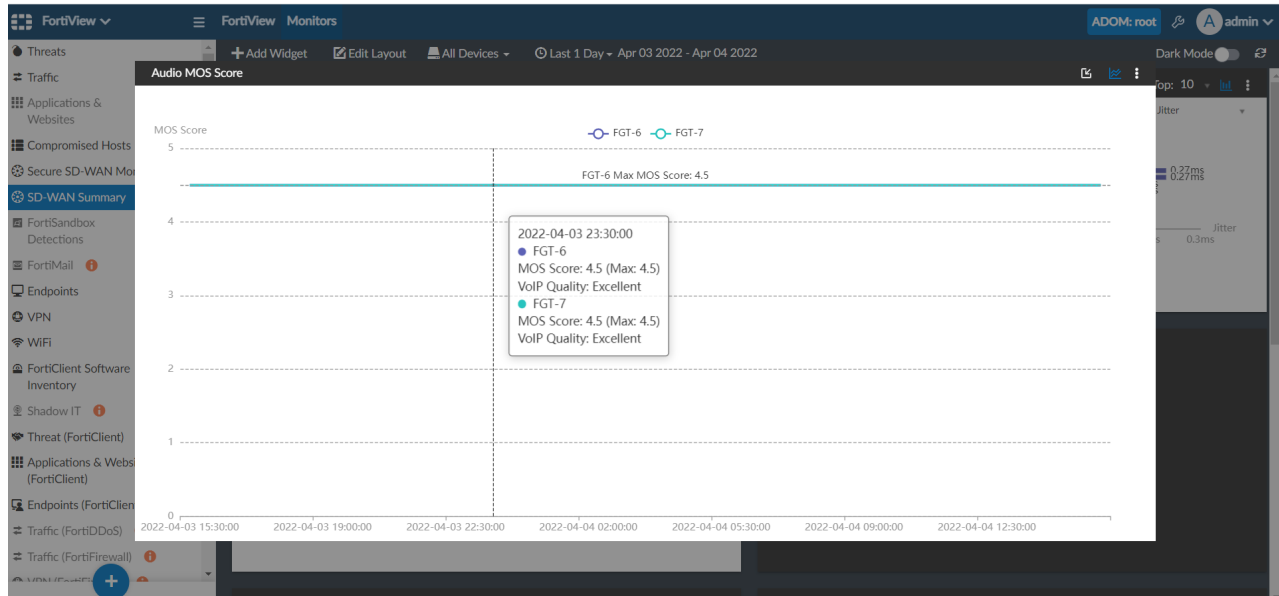
The widget includes a line graph of MOS score per device on the network.



3. Click a device in the legend to make it appear/disappear on the chart.  
 Greyed-out devices on the legend do not appear on the chart.



4. Hover your cursor over the chart to see a summary at that point.  
This summary includes the MOS score and the VoIP quality at that time.



To configure the FortiGate MOS codec and threshold in health check settings:

1. Access the FortiGate CLI.
2. Enter the following commands:
 

```
config system sdwan
config health-check
edit <name>
set server {string}
set sla-fail-log-period {integer}
set sla-pass-log-period {integer}
set members <seq-num1>, <seq-num2>, ...
set mos-codec [g711|g722|...]
config sla
edit <id>
set link-cost-factor {option1}, {option2}, ...
set mos-threshold {string}
next
end
```

For example:

```
config system sdwan
config health-check
edit "test_dc"
set server "10.200.1.1"
set sla-fail-log-period 15
set sla-pass-log-period 15
set members 1 2
set mos-codec g722
config sla
edit 1
set link-cost-factor latency jitter packet-loss mos
set mos-threshold "2.0"
next
```

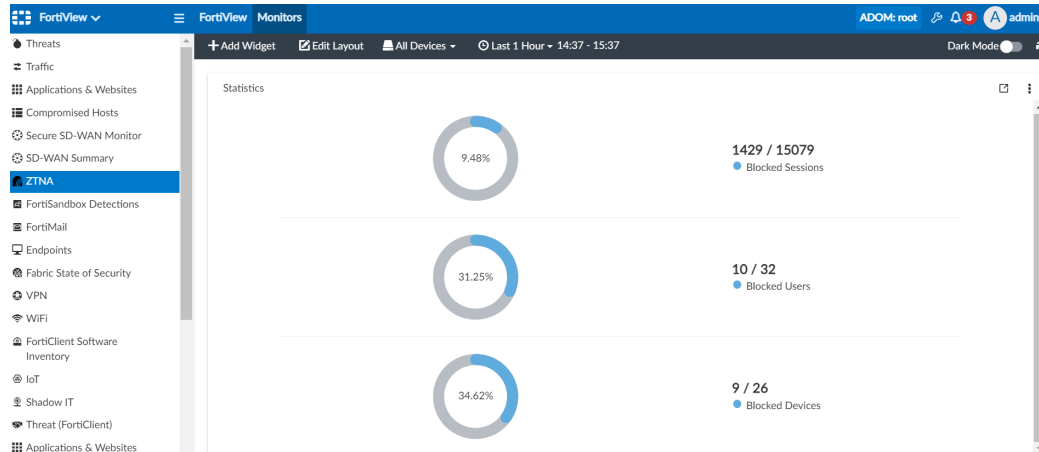
end

## Add ZTNA dashboard to FortiView

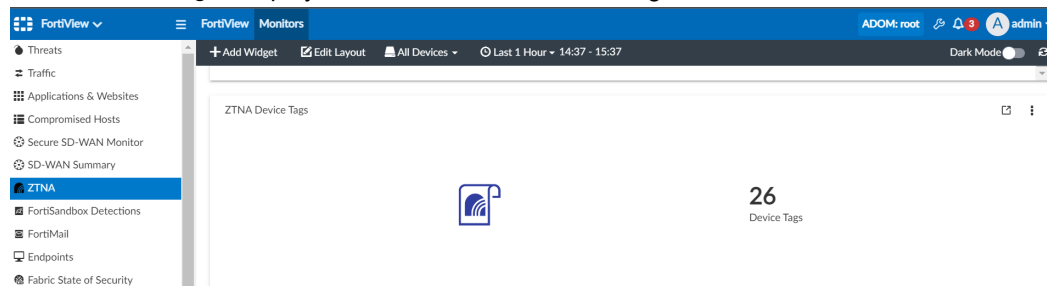
A ZTNA dashboard is added to *FortiView > Monitors*, providing visibility to ZTNA metrics.

This dashboard includes the following widgets:

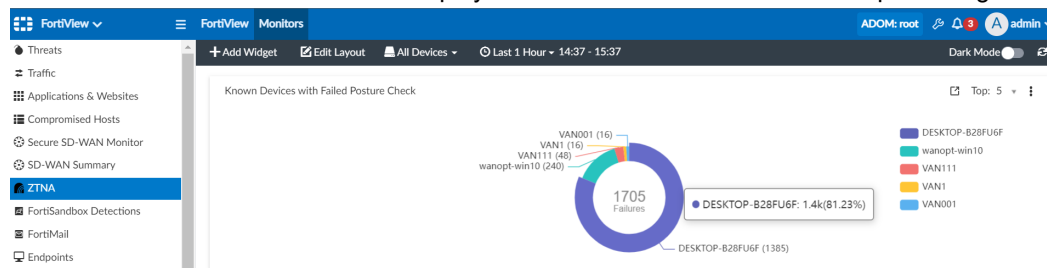
- **Statistics:** Displays the blocked sessions/total sessions, blocked users/total users, and blocked devices/total devices. The percentage of blocked sessions, users, and devices displays within their donut chart.



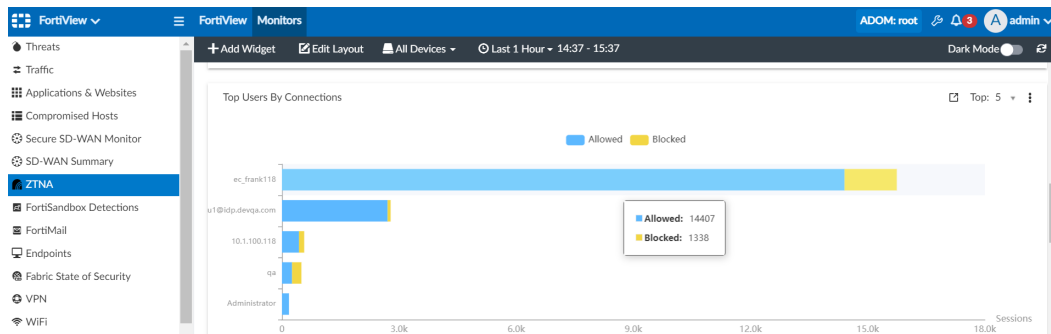
- **ZTNA Device Tags:** Displays the total number of device tags.



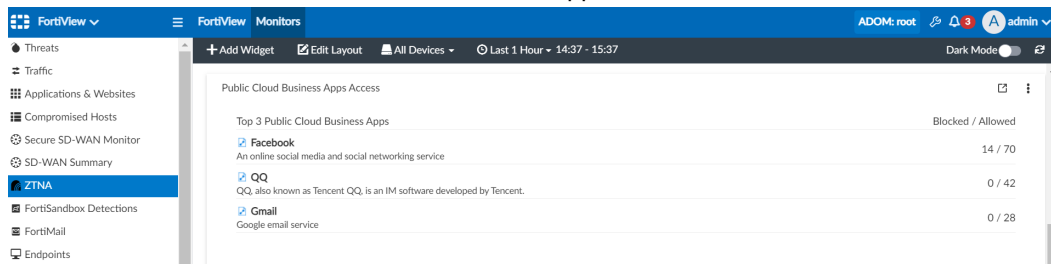
- **Known Devices with Failed Posture Check:** Displays the number of known devices with failed posture check by user. Mouse over the donut chart to display the related number devices and its percentage of the total in a tooltip.



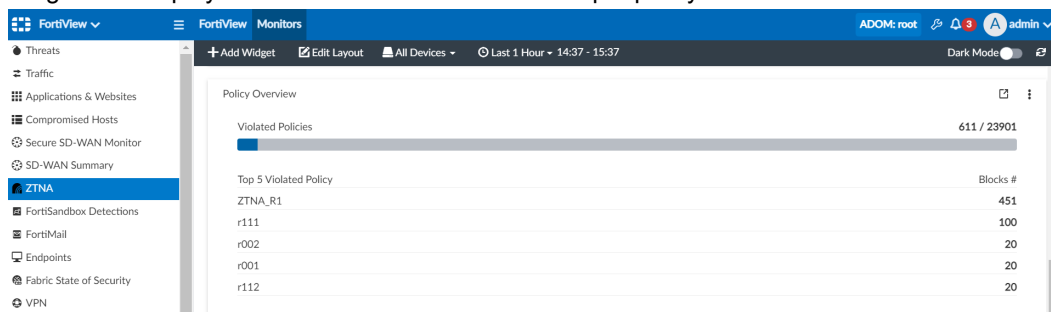
- **Top Users by Connections:** Displays the number of allowed and blocked sessions per user. Mouse over the bar chart to display the number of allowed and blocked sessions for that user in a tooltip.



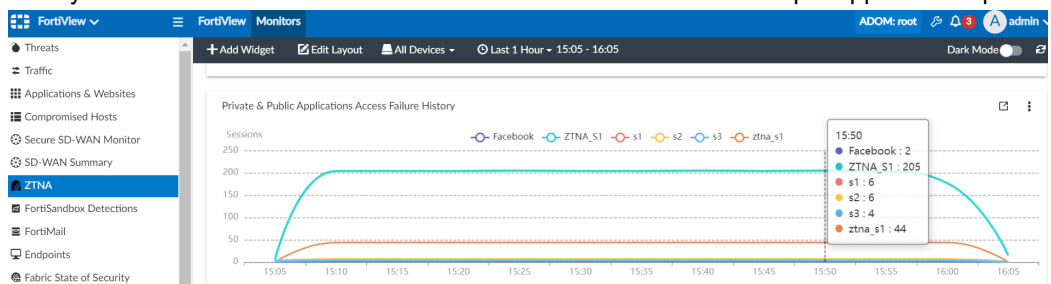
- **Public Cloud Business Apps Access:** Displays the top three public cloud business apps, including a description and the number of blocked/allowed sessions for each app.



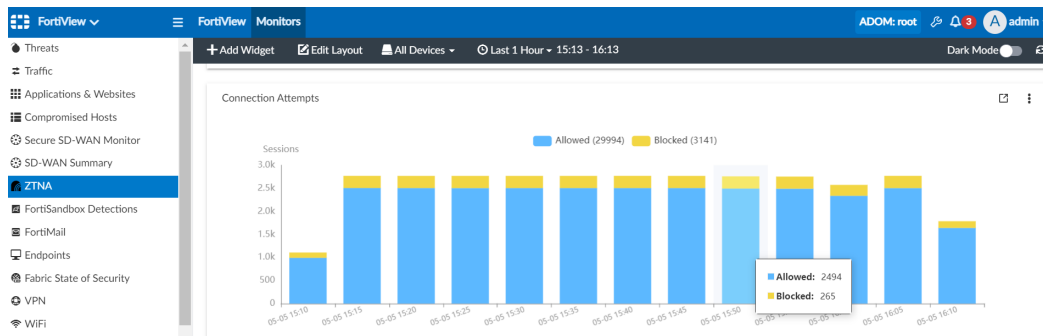
- **Policy Overview:** Displays the top five violated policies, including the total number of blocked/allowed sessions. This widget also displays the number of blocked sessions per policy.



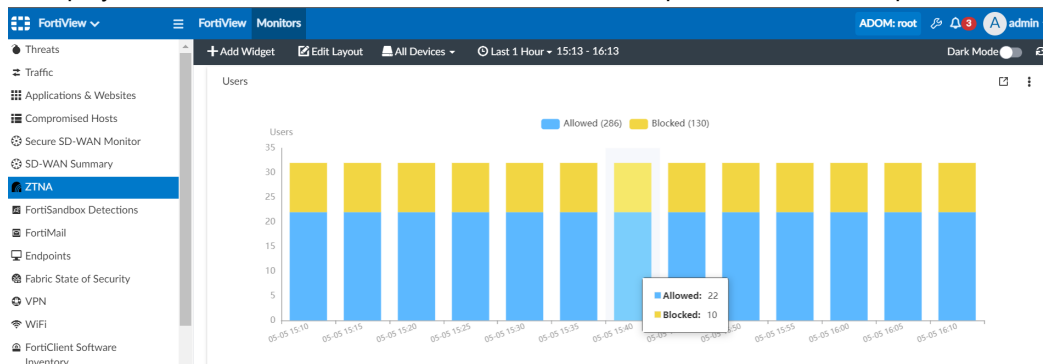
- **Private & Public Applications Access Failure History:** Displays the private and public applications with failed access history. Mouse over the line chart to view the number of access failures per app in a tooltip.



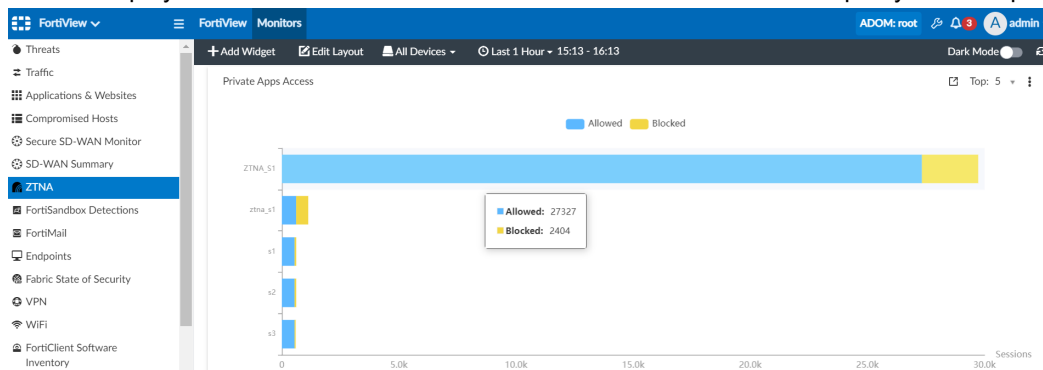
- **Connection Attempts:** Displays the number of allowed and blocked sessions within the selected time range. Mouse over the bar chart to display the number of allowed and blocked sessions at that specific time in a tooltip.



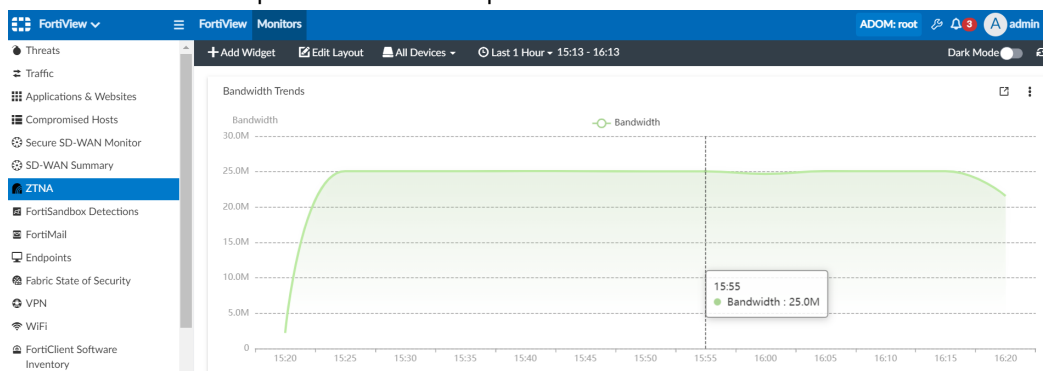
- **Users:** Displays the number of allowed and blocked users within the selected time range. Mouse over the bar chart to display the number of allowed and blocked users at that specific time in a tooltip.



- **Private Apps Access:** Displays the number of allowed and blocked sessions per access proxy. Mouse over the bar chart to display the number of allowed and blocked sessions for that access proxy in a tooltip.

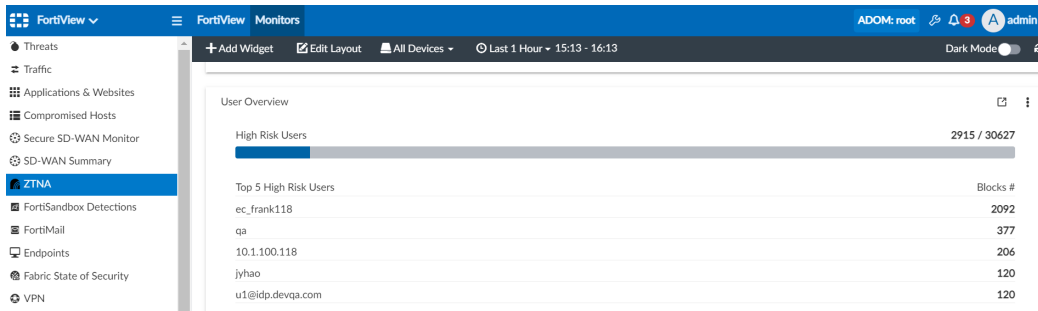


- **Bandwidth Trends:** Displays the bandwidth trends in the selected time range. Mouse over the line chart to display the bandwidth at that specific time in a tooltip.

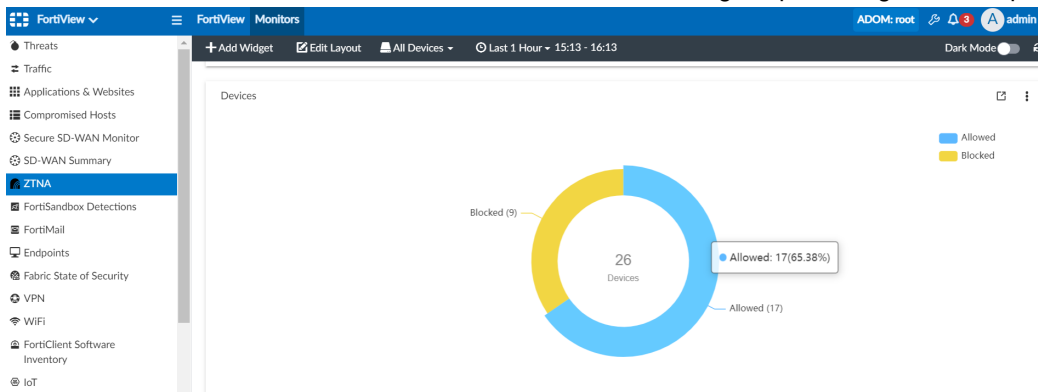




- **User Overview:** Displays the top five high risk users, including their combined blocked/total sessions and the total number of blocked sessions per user.



- **Devices:** Displays the blocked and allowed session number of the devices. Mouse over the donut chart to display the allowed session number or blocked session number, including the percentage in a tooltip.



## IoT visibility

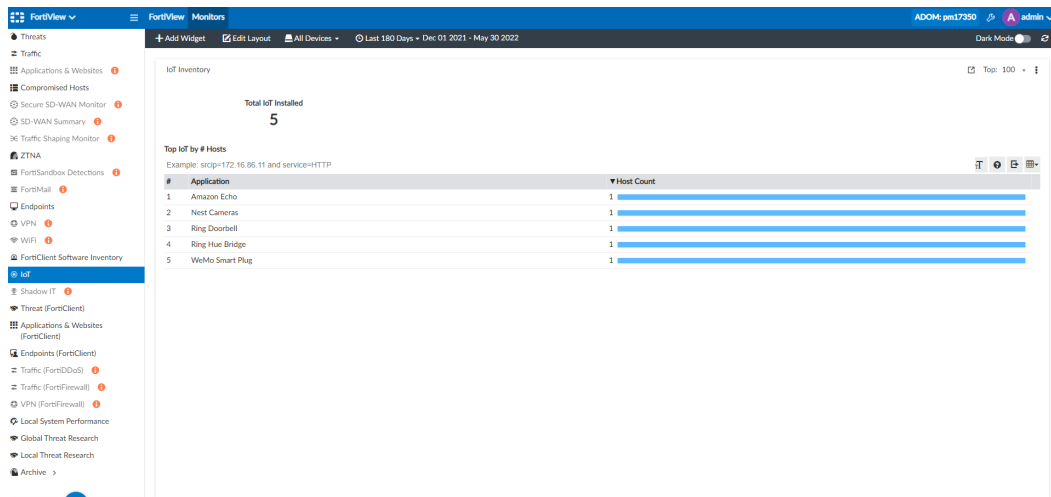
A dashboard is added to *FortiView > Monitors* for internet of things (IoT) device activity in FortiAnalyzer. IoT devices include smart devices, such as Amazon Echo.

This feature requires an IoT detection service license on FortiGate. Disable `local-sig` on FortiGate and configure the FortiGate to send logs to FortiAnalyzer so they are visible on the IoT dashboard.

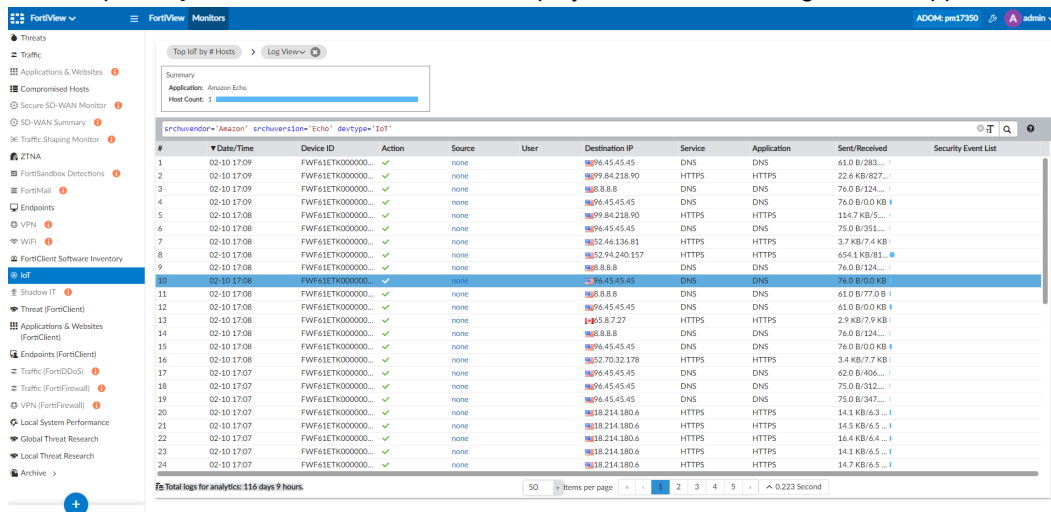
### To use the IoT dashboard:

1. Go to *FortiView > Monitors > IoT*.
2. From the *Device* dropdown, select the devices to filter the dashboard, as needed.
3. From the *Time* dropdown, select the time period to filter the dashboard, as needed.

The *IoT Inventory* widget displays the total number of IoT applications installed. This widget also includes a table of the *Top IoT by # Hosts*, which displays the top applications' name and host count.



4. In the *Top IoT by # Hosts* table, click a row to display the related traffic logs for that application.



## Traffic shaping charts - 7.2.1

The *Traffic Shaping Monitor* dashboard is added to *FortiView > Monitors*.

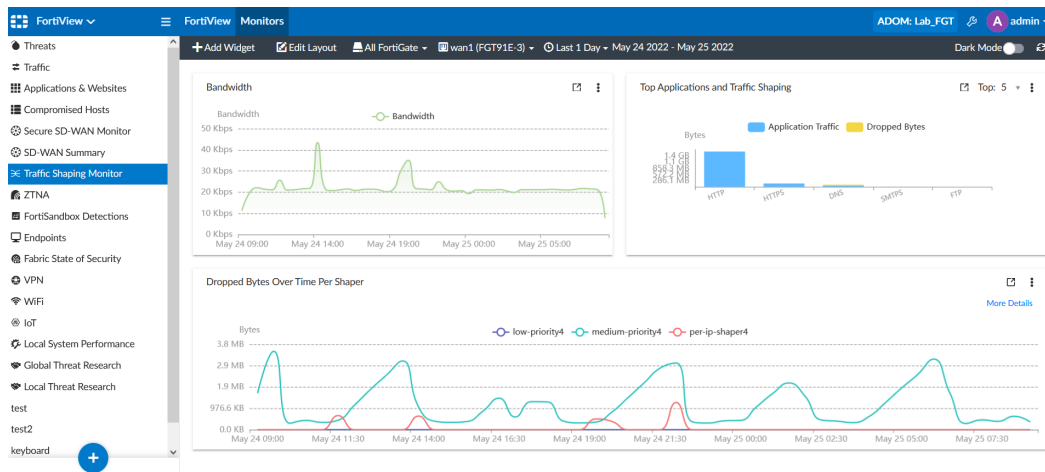
This dashboard includes the following widgets:

- **Bandwidth:** Displays the bandwidth of traffic shapers over time in a line chart.
- **Top Applications and Traffic Shaping:** Displays the traffic volume and dropped bytes for the top applications in a stacked bar chart.
- **Dropped Bytes Over Time Per Shaper:** Displays the dropped bytes for different traffic shapers on a selected interface over a period of time in a line chart.

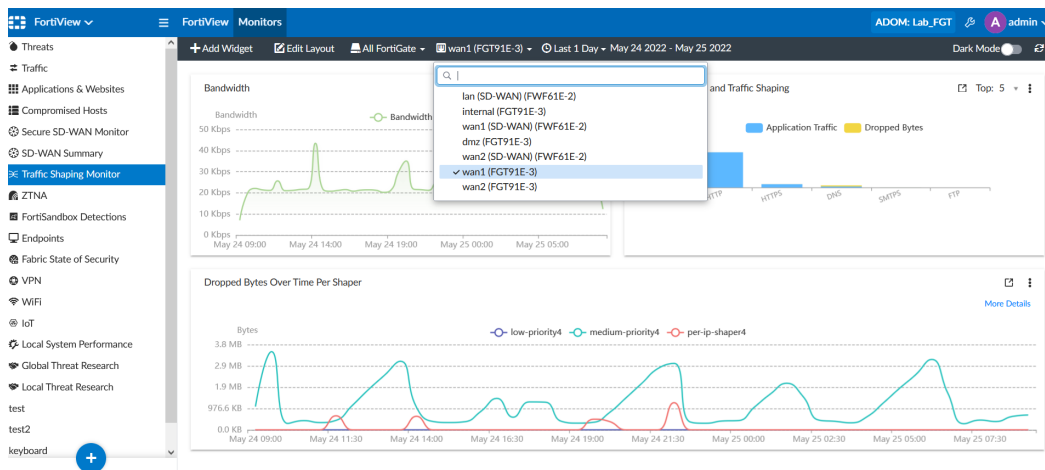


To use the *Traffic Shaping Monitor*, you must configure per-IP traffic shaper and shared traffic shaper on the FortiGate device. Then, configure a traffic shaping policy. For more information, see the [FortiGate Administration Guide](#).

To use these widgets, go to *FortiView > Monitors > Traffic Shaping Monitor*.

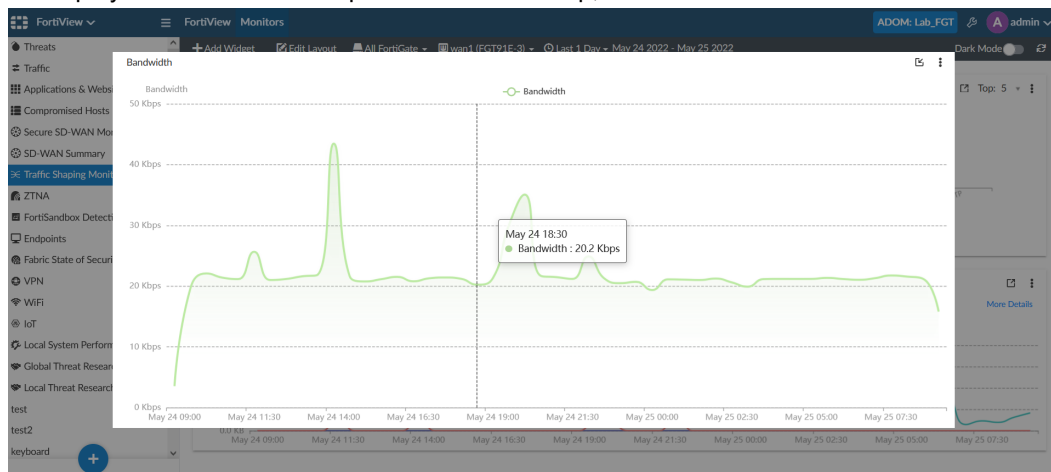


From the toolbar, select the devices, the traffic shaping interface, and a time range for the monitor. In the image below, the user selects *wan1 (FGT91E-3)* as the traffic shaping interface.



To use the **Bandwidth** widget:

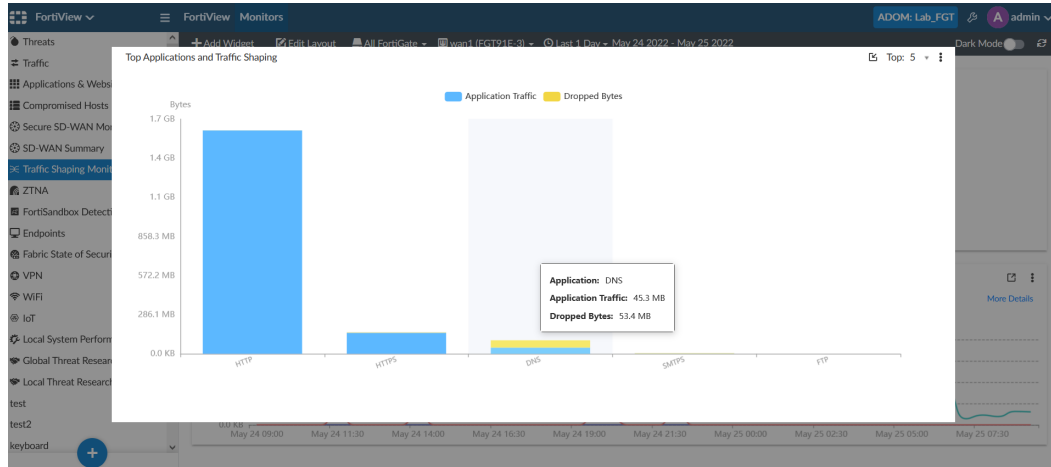
1. To display the bandwidth at a specific time in a tooltip, mouse over the line chart.



You can also click the bandwidth icon in the legend to hide/show the corresponding line in the chart.

**To use the *Top Applications and Traffic Shaping* widget:**

1. From the *Top* dropdown, select the number of top applications (5/10/15/20) to display in the widget . The widget displays the top five applications by default.
2. To display a summary of application traffic and dropped bytes in a tooltip, mouse over the stacked bar chart.



*Application Traffic* and *Dropped Bytes* can be hidden/shown in the bar chart by click the corresponding icon in the legend.

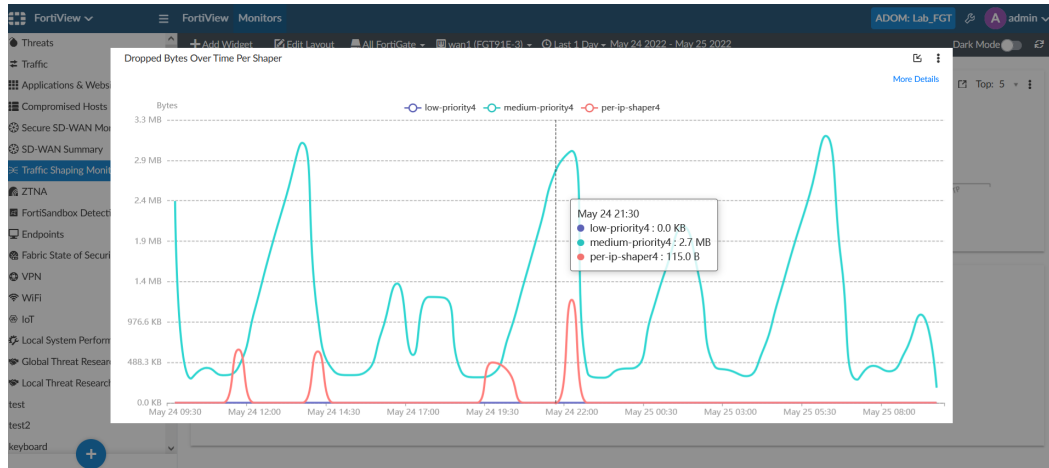
3. To display the *Application Users* table view, click a bar in the chart. This view includes a summary of the application traffic, including the number of sessions and bytes (sent/received) by user.

#	User Name	IP	Sessions	Bytes (Sent/Received)
1	10.2.175.100	10.2.175.100	4,078	190.8 KB/342.8 KB
2	10.2.175.106	10.2.175.106	2,783	206.2 KB/289.3 KB
3	10.2.175.107	10.2.175.107	1,993	131.7 KB/186.0 KB
4	10.2.175.101	10.2.175.101	905	128.2 KB/148.5 KB
5	10.2.175.108	10.2.175.108	368	924.6 KB/2.3 MB

4. To return to the widget, click *Top Applications and Traffic Shaping*.

## To use the *Dropped Bytes Over Time Per Shaper* widget:

1. To display a summary of dropped bytes per shaper in a tooltip, mouse over the line chart.



2. Click a shaper in the legend to hide/show it in the line chart. Greyed-out shapers in the legend are hidden in the line chart.
3. Click *More details* to display the *Traffic Shaping Policy Hits* table view. This table includes the total sessions and bytes (sent/received) by shaping policy.

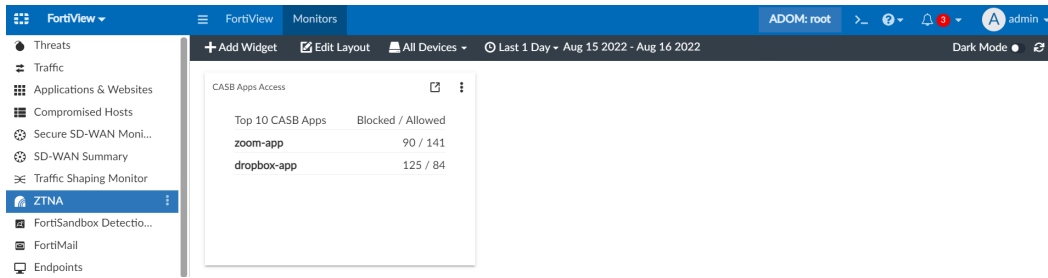
#	Shaping Policy	Source Interface	Shared Shaper	Reverse Shaper	Per IP Shaper	Service	Applications	Sessions	Bytes (Sent/Received)
1	1	wan2			per-ip-shaper4	HTTP/HTTPS	HTTP HTTPS	102,721	199.5 MB/1.5 GB
2	3	wan2	medium-priority4	medium-priority4		DNS.SMTPS	DNS SMTPS	10,627	20.3 MB/26.6 MB
3	2	wan2	low-priority4	low-priority4		FTP	FTP	1	1.3 KB/1.4 KB

4. To return to the chart, click *Dropped Bytes Over Time Per Shaper*. Note that shared shapers, reverse shapers, and per-ip shapers are supported in this widget.

## CASB Apps Access widget - 7.2.1

The new *CASB Apps Access* widget is added in *FortiView > Monitors > ZTNA*.

This widget lists the top 10 inline CASB applications, including a count of the *Blocked / Allowed* sessions per application. The CASB application name in this chart is the "saasname" in ZTNA traffic logs.



## Auto-refresh on FortiSoC dashboard elements - 7.2.2

An auto-refresh dropdown is added to all FortiSoC dashboard, including *Playbooks*, *Incidents*, and *Events*. From each dashboard toolbar, the auto-refresh interval can be set to:

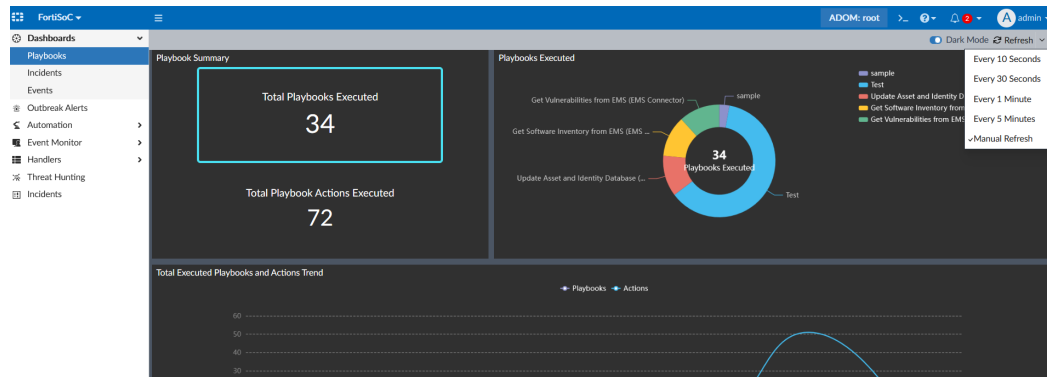
- *Every 10 Seconds*
- *Every 30 Seconds*
- *Every 1 Minute*
- *Every 5 Minutes*
- *Manual Refresh*

By default, the auto-refresh interval is set to *Manual Refresh*. With this setting selected, you must click *Refresh* in the toolbar to refresh the dashboard when needed.

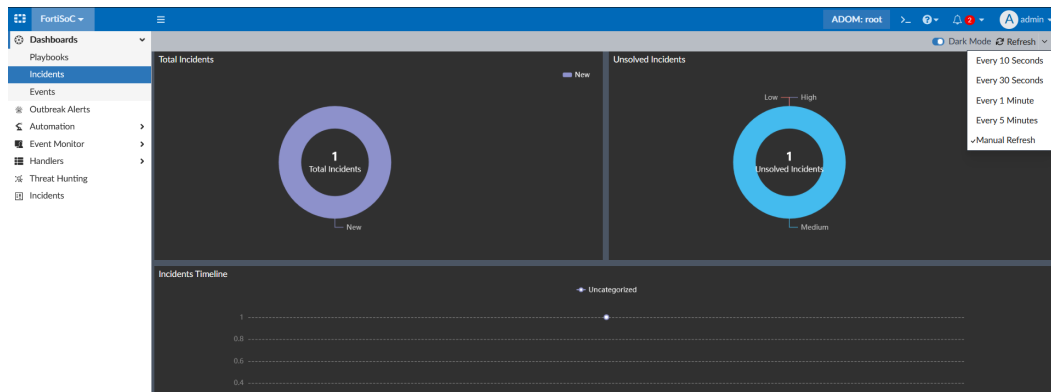
When another auto-refresh interval is selected, the dashboard will automatically refresh at the interval time. Alternatively, you can click *Refresh* to refresh the dashboard before the interval time is reached.

See below for images of the auto-refresh dropdown in the FortiSoC dashboards:

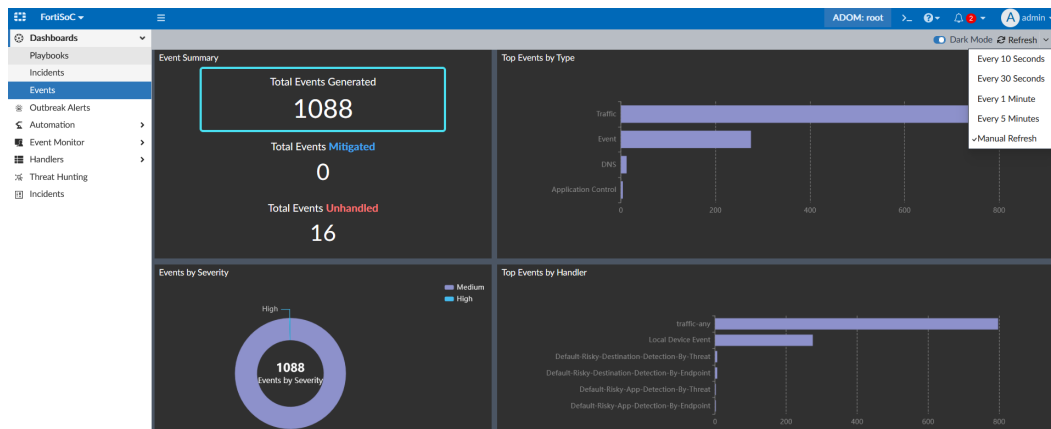
- *FortiSoC > Dashboards > Playbooks*



- *FortiSoC > Dashboards > Incidents*



### • FortiSoC > Dashboards > Events



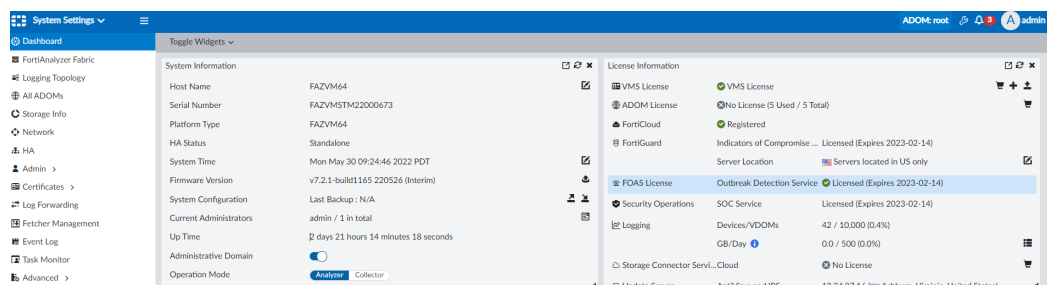
## Others

This section lists the new features added to FortiAnalyzer for other topics related to security operations:

- [Rename Outbreak Alerts Service to Outbreak Detection Service on page 55](#)

## Rename Outbreak Alerts Service to Outbreak Detection Service

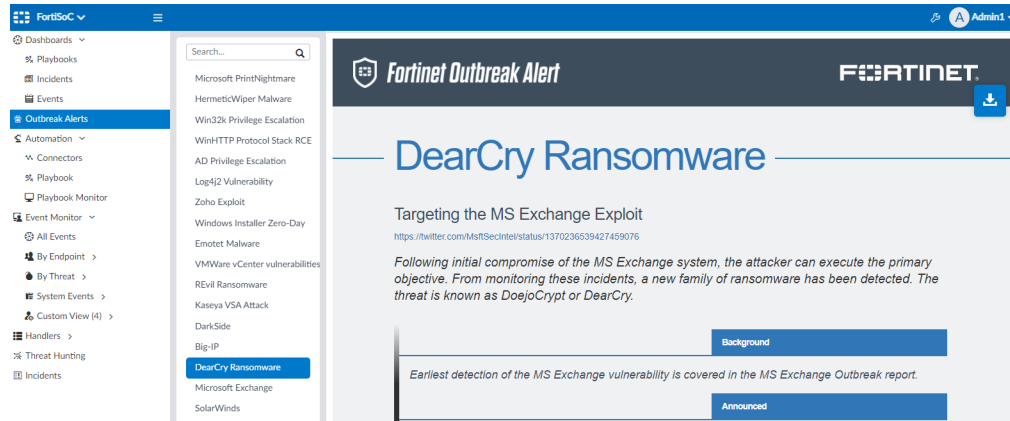
The Outbreak Alerts Service in FortiAnalyzer is renamed to Outbreak Detection Service. See examples from the GUI and CLI below.



```
FAZYM64 # dia license list
```

Name	Status	Expiry	Description
PBDS	Valid	2023-02-14	post breach detection
SCPC	No License	N/A	cloud storage service
SOAR	Valid	2023-02-14	SOAR and SIEM bundle service
FOAS	Valid	2023-02-14	FAZ Outbreak Detection Service

There is no change to functionality for this service. The FortiAnalyzer Outbreak Detection Service is a licensed feature that allows FortiAnalyzer administrators to view outbreak alerts and automatically download related event handlers and reports from FortiGuard. When FortiAnalyzer has a valid license for the Outbreak Detection Service, outbreak alerts from Fortinet are displayed in *FortiSoC > Outbreak Alerts* from any ADOM.



## To view outbreak event handlers and reports:

### 1. Go to *FortiSoC > Handlers > Event Handler List*.

Event handlers created by the FortiAnalyzer Outbreak Detection Service are displayed with the Outbreak Alert prefix.

Status	Name	Filters	Devices	Send Alert to	Events	Included Subnets	Excluded Subnets
✓	Outbreak Alert - VMware vCenter Vulnerability Detection	> 2 Filters	All Devices				
✓	Outbreak Alert - HermeticWiper Malware Event-Handler	> 4 Filters	All Devices				
✓	Outbreak Alert - DarkSide Ransomware Detection	> 11 Filters	All Devices				
✓	Outbreak Alert - MS.Exchange-HAFNIUM Attack Detection	> 5 Filters	All Devices				
✓	Outbreak Alert - Big-IP Attack Detection	> 2 Filters	All Devices				
✓	Outbreak Alert - REvil Ransomware Detection	> 3 Filters	All Devices				
✓	Outbreak Alert - DearCry Ransomware Detection	> 3 Filters	All Devices				
✓	Outbreak Alert - Emotet Malware Event-Handler	> 4 Filters	All Devices				
✓	Outbreak Alert - Windows Installer Zero-Day Event-Handler	> 3 Filters	All Devices				
✓	Outbreak Alert - Zoho Exploit Event-Handler	> 3 Filters	All Devices				
✓	Outbreak Alert - Log4j2 Vulnerability Event-Handler	> 2 Filters	All Devices				
✓	Outbreak Alert - AD Privilege Escalation Event-Handler	> 2 Filters	All Devices				
✓	Outbreak Alert - Windows HTTP Protocol Stack RCE Event-Handler	> 4 Filters	All Devices				
✓	Outbreak Alert - Win32k Privilege Escalation Event-Handler	> 3 Filters	All Devices				
✓	Outbreak Alert - PrintNightmare Vulnerability Detection	> 2 Filters	All Devices				
✓	Outbreak Alert - Kaseya VSA Vulnerability for CVE-2021-30116	> 3 Filters	All Devices				
✓	Outbreak Alert - SolarWinds Compromised Host Detection	> 18 Filters	All Devices				
✓	Unique_Count_IP_PortScan	> 1 Filter	All Devices		18		

### 2. Go to *Reports > All Reports*.

The *Outbreak Alert Reports* folder includes available reports from the FortiAnalyzer Outbreak Detection Service.



Reports

Generated Reports

Report Definitions

All Reports

Templates

Chart Library

Macro Library

Datasets

Advanced

Language

Output Profile

Report Calendar

Run Report

Report

Folder

More

Show Scheduled Only

Column Settings

Search

	Title	Language	Cache Status	Time Period	Devices	Schedule	Out
<input type="checkbox"/>	Application						
<input type="checkbox"/>	Detailed User Report						
<input type="checkbox"/>	FortClient Report						
<input checked="" type="checkbox"/>	Outbreak Alert Reports						
<input checked="" type="checkbox"/>	Outbreak Alert - AD Privilege Escalation Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - DarkSide Ransomware Detection Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - DarkCry Ransomware Detection Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - Emotet Malware Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - FS Big-IP Attack Detection Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - HermeticWiper Malware Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - Kaseya VSA Vulnerability for CVE-2021-30116 Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - Log4j2 Vulnerability Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - MS Exchange-HAFNIUM Attack Detection Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - PrintNightmare Vulnerability for CVE-2021-34527 Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - Revil Ransomware Detection Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - SolarWinds Compromised Host Detection Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - VMware vCenter Vulnerability Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - Win32k Privilege Escalation Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - Windows HTTP Protocol Stack RCE Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - Windows Installer Zero-Day Report	English					
<input checked="" type="checkbox"/>	Outbreak Alert - Zoho Exploit Report	English					
<input type="checkbox"/>	Web						
<input type="checkbox"/>	360-Degree Security Review	English					
<input type="checkbox"/>	Admin and System Events Report	English					

# Log and Report

This section lists the new features added to FortiAnalyzer for logs and reports:

- [Logging on page 58](#)
- [Reports on page 69](#)
- [Others on page 93](#)

## Logging

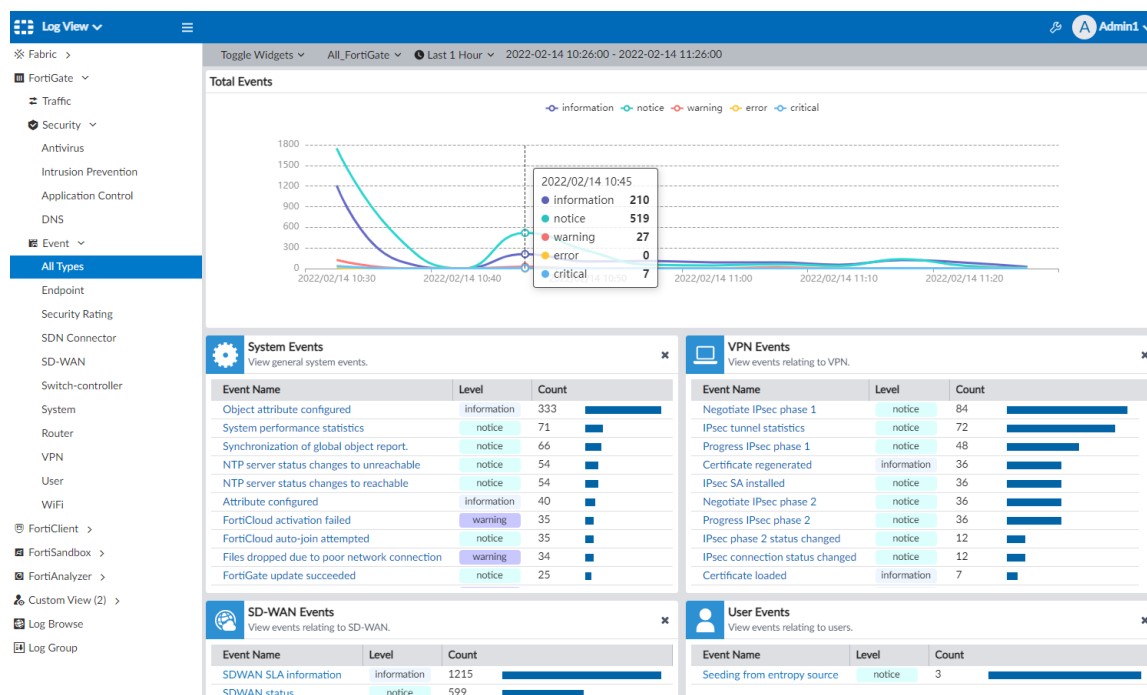
This section lists the new features added to FortiAnalyzer for logging:

- [Summary dashboard for event logs on page 58](#)
- [Log caching enhancement on page 62](#)
- [FortiNDR logging and reporting enhancements 7.2.1 on page 64](#)
- [Security events consolidated page 7.2.1 on page 66](#)

### Summary dashboard for event logs

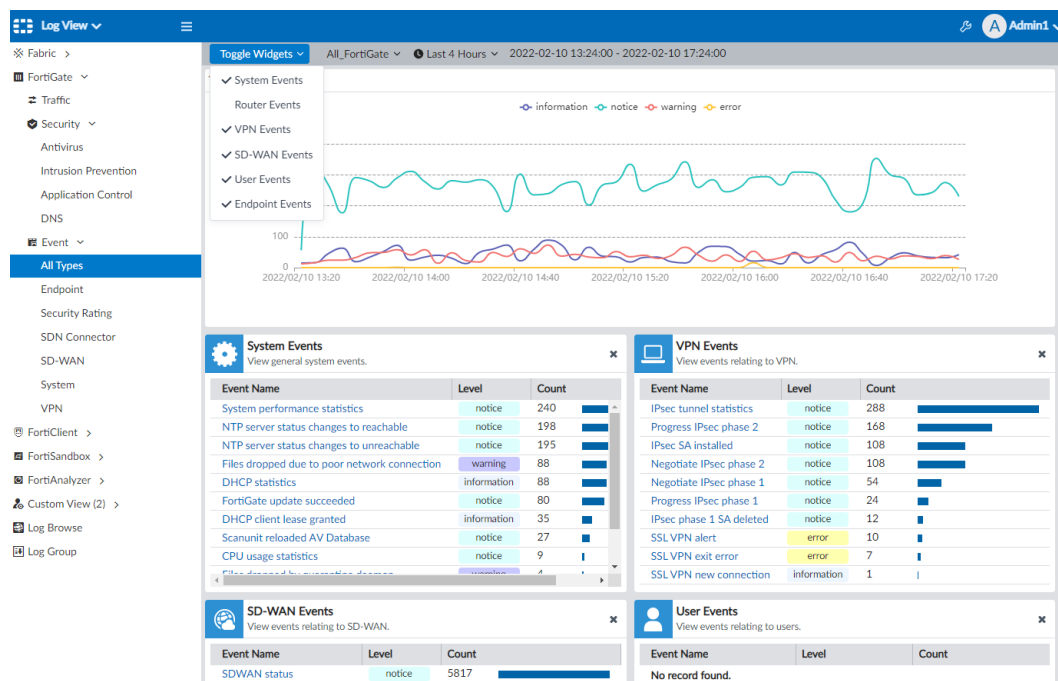
A new event log dashboard is added in *Log View > FortiGate > Events > All Types*. This dashboard displays total counts for the event logs by type, name, and level. You can choose which types of event logs display on the dashboard by toggling the widgets on/off. You can also filter the dashboard by FortiGate device(s) and time frame for the event logs.

The *Total Events* widget in this dashboard displays a line chart of event logs by level. Hover your cursor over the line chart to display a summary at that point.



### To toggle widgets on the dashboard:

1. Go to **Log View > FortiGate > Event > All Types**.
2. From the **Toggle Widgets** dropdown, select the widgets to display on the dashboard.  
You can also toggle widgets off by clicking **X** on the widget.

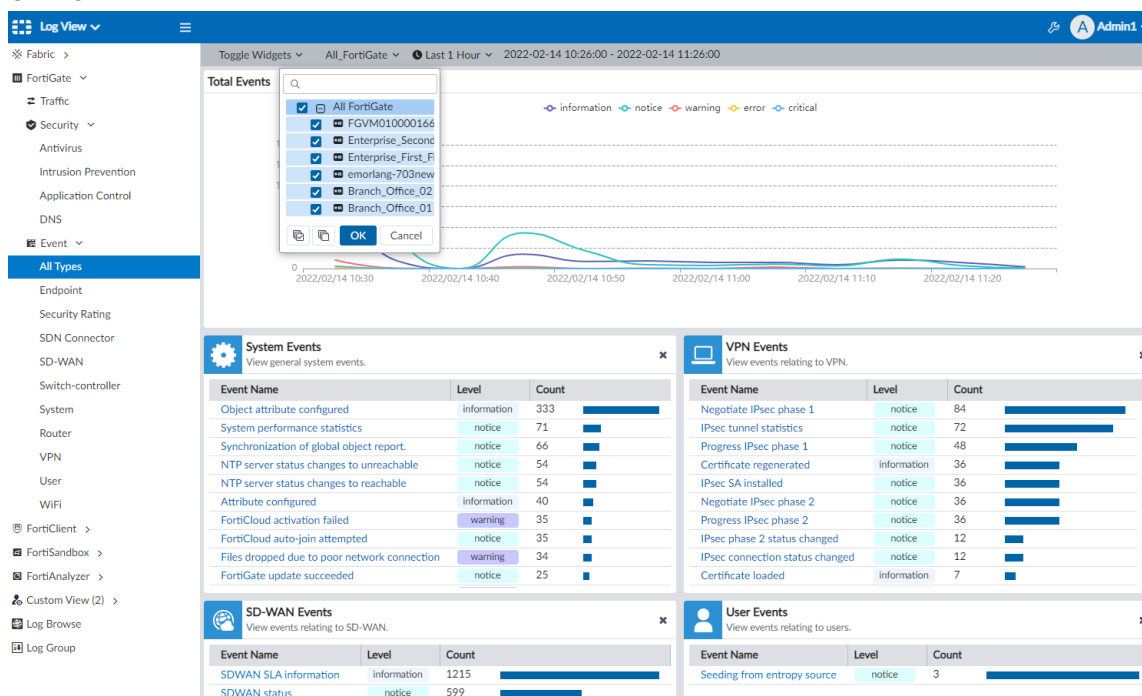




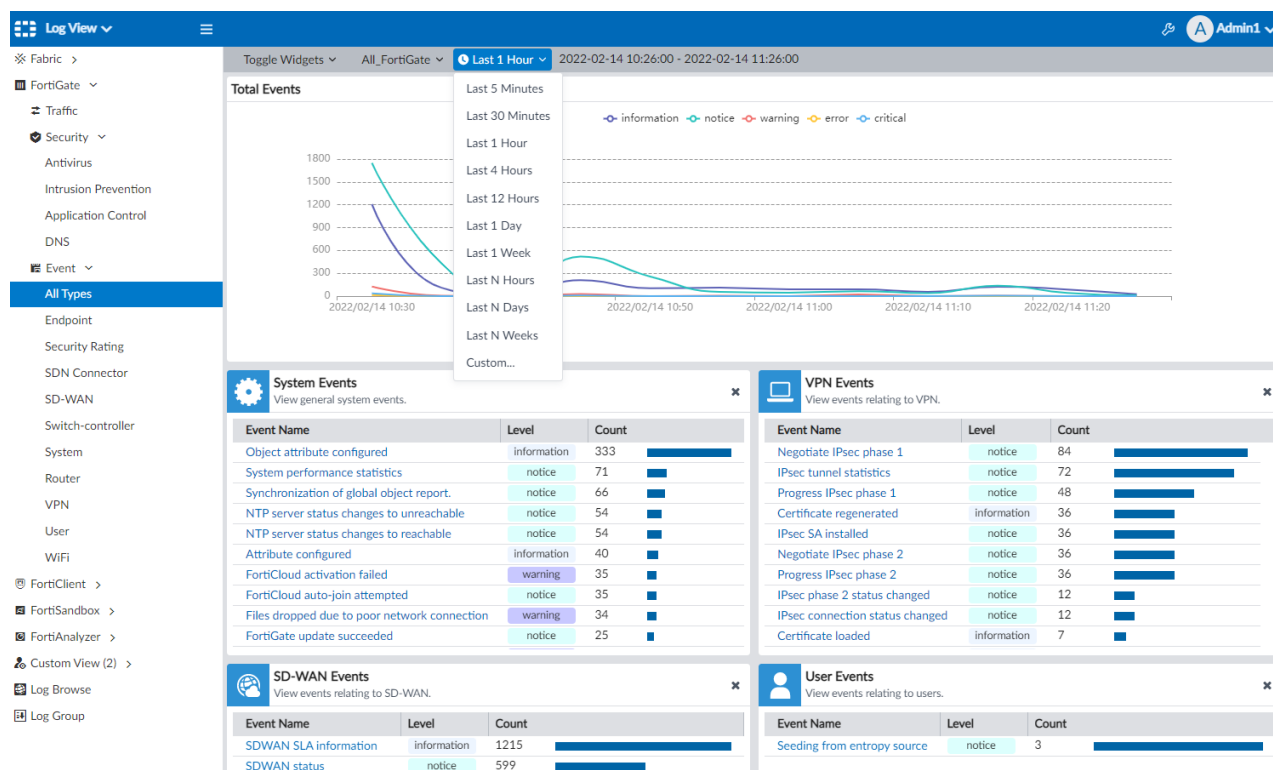
The *Total Events* widget cannot be toggled off.

### To filter the dashboard:

1. From the device dropdown, select the FortiGate devices to include for the dashboard.
2. Click **OK**.

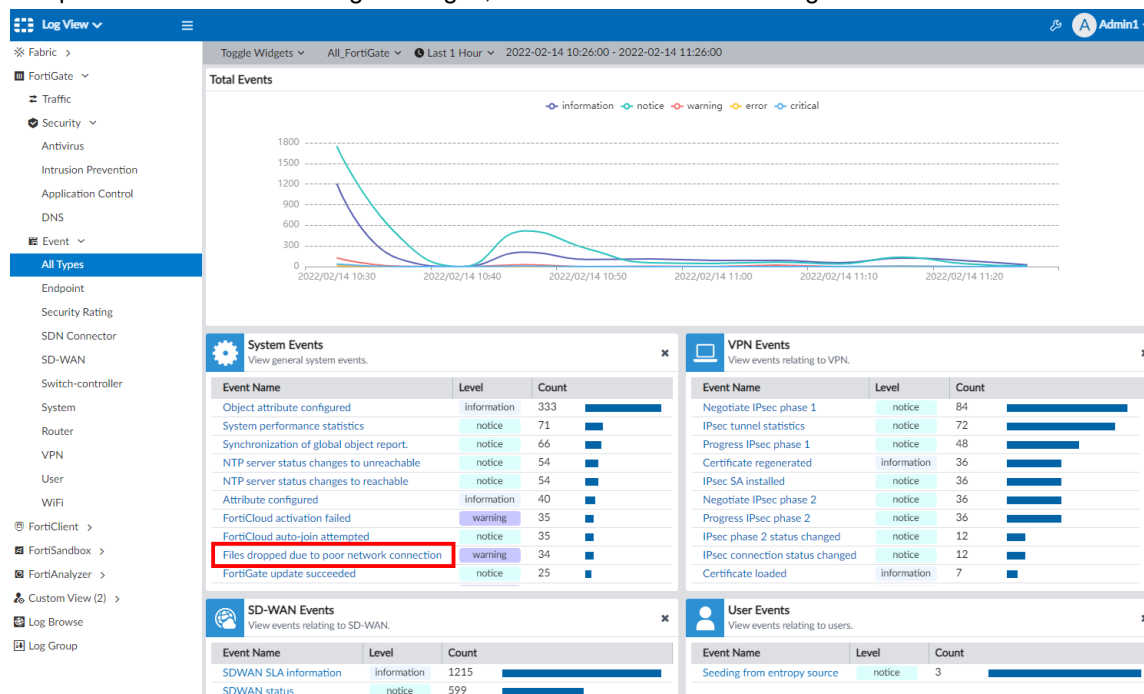


3. From the time dropdown, select the time frame for the dashboard.  
You can select *Custom...* to set a custom time frame.



To open a list view of log messages from the dashboard:

1. To open a list view of related log messages, click an event name in a widget.



The list of event logs is filtered by the devices and time frame that you selected on the dashboard.

#	Date/Time	Level	Device ID	Message	User
1	11:07:32	warning	FGVM02TM21010777	1 files were dropped by quard to ...	
2	11:07:32	warning	FGVM02TM21010777	1 files were dropped by quard to ...	
3	11:07:32	warning	FGVM02TM21010777	1 files were dropped by quard to ...	
4	11:07:32	warning	FGVM02TM21010777	1 files were dropped by quard to ...	
5	11:07:25	warning	FGVM02TM21012920	1 files were dropped by quard to ...	
6	11:07:25	warning	FGVM02TM21012920	1 files were dropped by quard to ...	
7	11:07:24	warning	FGVM02TM21012920	1 files were dropped by quard to ...	
8	11:07:23	warning	FGVM02TM21012920	1 files were dropped by quard to ...	
9	11:07:23	warning	FGVM02TM21012920	1 files were dropped by quard to ...	
10	11:07:22	warning	FGVM02TM21012633	1 files were dropped by quard to ...	
11	11:07:22	warning	FGVM02TM21012633	1 files were dropped by quard to ...	
12	11:07:22	warning	FGVM02TM21012633	1 files were dropped by quard to ...	
13	11:07:22	warning	FGVM02TM21012633	1 files were dropped by quard to ...	
14	11:07:16	warning	FGVM02TM21011279	1 files were dropped by quard to ...	
15	11:07:16	warning	FGVM02TM21011279	1 files were dropped by quard to ...	
16	11:07:16	warning	FGVM02TM21011279	1 files were dropped by quard to ...	
17	11:07:16	warning	FGVM02TM21011279	1 files were dropped by quard to ...	
18	10:46:13	warning	FGVM02TM21010777	1 files were dropped by quard to ...	
19	10:46:13	warning	FGVM02TM21010777	1 files were dropped by quard to ...	
20	10:46:13	warning	FGVM02TM21010777	1 files were dropped by quard to ...	
21	10:46:13	warning	FGVM02TM21010777	1 files were dropped by quard to ...	
22	10:46:13	warning	FGVM02TM21011279	1 files were dropped by quard to ...	
23	10:46:13	warning	FGVM02TM21011279	1 files were dropped by quard to ...	
24	10:46:13	warning	FGVM02TM21011279	1 files were dropped by quard to ...	
25	10:46:13	warning	FGVM02TM21011279	1 files were dropped by quard to ...	
26	10:46:12	warning	FGVM02TM21012633	1 files were dropped by quard to ...	
27	10:46:12	warning	FGVM02TM21012633	1 files were dropped by quard to ...	
28	10:46:12	warning	FGVM02TM21012633	1 files were dropped by quard to ...	
29	10:46:12	warning	FGVM02TM21012633	1 files were dropped by quard to ...	
30	10:45:47	warning	FGVM02TM21012920	1 files were dropped by quard to ...	

Total logs for analytics: 1 hour. 50 items per page 1 0.096 Second

## Log caching enhancement

FortiAnalyzer log caching mechanism in reliable mode is enhanced to prevent Fortigate log loss during connection interruptions.

Log sync logic guarantees that no logs are lost due to connection issues when reliable mode is enabled on the FortiGate device. If connection is lost between the FortiAnalyzer and FortiGate device, logs will be cached and sent to FortiAnalyzer once the connection resumes.



Reliable mode is disabled by default on FortiGate devices.

### To configure the FortiGate device:

1. Configure the FortiGate device to send logs to FortiAnalyzer.
2. In the FortiGate CLI, enter the following commands to confirm *reliable* is enabled:

```
config log fortianalyzer2 setting
show
```

For example:

```
config log fortianalyzer2 setting
show
config log fortianalyzer2 setting
set status enable
set server "10.2.169.54"
set serial "FAZ-VM0000000001"
set upload-option realtime
set reliable enable
```

end

3. In the FortiGate CLI, enter the following commands to confirm the value of `logsync_enabled` is 1:

```
diagnose test application fgtlogd 1
```

For example:

```
diagnose test application fgtlogd 1

faz2: global , enabled
  server=10.2.169.54, realtime=1, ssl=1, state=connected
  server_log_status=Log is allowed.,
  src=, mgmt_name=FGh_Log_root_10.2.169.54, reliable=1, sni_prefix_type=none,
  required_entitlement=none, region=ca-west-1,
  logsync_enabled:1, logsync_conn_id:131071, seq_no:257
  status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_verified=Y
  SNs: last sn update:2097 seconds ago.
    Sn list:
      (FAZ-VM0000000001,age=2097s) (FAZ-VMJY00000004,age=2097s)
    queue: qlen=0.
  filter: severity=6, sz_exclude_list=0
```

### To confirm cached logs are sent when connection is lost/resumed between FortiGate and FortiAnalyzer:

In this example, the FortiGate device has already been configured according to the steps above. When connection is lost between the FortiGate and FortiAnalyzer device, logs are cached on the FortiGate until connection resumes. Once connection resumes, the cached logs are sent to the FortiAnalyzer.

1. While connection between the FortiGate and FortiAnalyzer is established, check the log sequence number on the OFTP connection.

In the FortiAnalyzer CLI, enter the following command:

```
diagnose test application oftpd 3
#  DEVICE  CONN  HOSTNAME  IP  UPTIME  IDLETIME  #PKTS
-----
--
1  FGT40FTK20025663  131071: 257  FortiGate-40F  10.3.169.1  31m14s  4s  620
```

The **CONN** column has been added to record the connection ID and log sequence number. In this example, the connection ID is 131071 and the sequence number is 257.

2. When the connection between the FortiGate and FortiAnalyzer is lost, check the log sequence number on the OFTP connection.

In the FortiAnalyzer CLI, enter the following command:

```
diagnose test application oftpd 3
#  DEVICE  CONN  HOSTNAME  IP  UPTIME  IDLETIME  #PKTS
-----
--
1  FGT40FTK20025663  131071: 257  FortiGate-40F  10.3.169.1  35m14s  244s  620
```

While the connection is lost, logs generated on the FortiGate device will be stored in its memory queue. The log sequence number on the OFTP connection will not increase. In this example, the log sequence number has remained at 257.

3. When the connection between the FortiGate and FortiAnalyzer device resumes, check logs on the FortiGate device.

In the FortiGate CLI, enter the following command:

```
diagnose test application fgtlogd 41

cache maximum: 100573388(95MB) objects: 37 used: 25788(0MB) allocated: 29440(0MB)

VDOM:root
```

```

Memory queue for: global-faz
queue:
  num:0 size:0(0MB) total size:25788(0MB) max:100573388(95MB) logs:0
Confirm queue for: global-faz
queue:
  num:25 size:17382(0MB) total size:25788(0MB) max:100573388(95MB) logs:81
Memory queue for: global-faz2
queue:
  num:0 size:0(0MB) total size:25788(0MB) max:100573388(95MB) logs:0
Confirm queue for: global-faz2
queue:
  num:12 size:8406(0MB) total size:25788(0MB) max:100573388(95MB) logs:40

```

The confirm queue on the FortiGate device shows all the logs that are waiting to be confirmed and cleared. Once the confirm queue displays 0, all of the cached logs have been sent to the FortiAnalyzer device.

- Once the logs have been confirmed and cleared from the FortiGate device, check the log sequence number on the OFTP connection.

In the FortiAnalyzer CLI, enter the following command:

```

diagnose test application oftpd 3
#  DEVICE  CONN  HOSTNAME  IP  UPTIME  IDLETIME  #PKTS
-----

```

```

1  FGT40FTK20025663  131071: 308  FortiGate-40F  10.3.169.1  36m23s  6s  635

```

Once the cached logs have been sent to the FortiAnalyzer device, the log sequence number increases. In this example, the log sequence number has increased to 308.

## FortiNDR logging and reporting enhancements - 7.2.1

The following enhancements are introduced for FortiNDR devices:

- In *Log View*, support is added for log type: *ndr*
- In *FortiSOC*, support is added for FortiNDR as log device type
- In *Reports*, the *FortiNDR Network Anomalies Report* and additional datasets are added

See below for more details.

A new log type is added for the FortiNDR device. These logs can be found in *Log View > FortiNDR > NDR*.

#	Date/Time	Device ID	Type	Sub Type	Severity	Application Layer Protocol	Cipher	Bel
1	10:47:57	FAIVMS0000000000	ndr	Encrypted	critical	OTHER	TLS_AES_256_GCM_SHA384	
2	10:47:52	FAIVMS0000000000	ndr	Encrypted	critical	OTHER	TLS_AES_256_GCM_SHA384	
3	10:47:47	FAIVMS0000000000	ndr	Encrypted	critical	OTHER	TLS_AES_256_GCM_SHA384	
4	10:47:42	FAIVMS0000000000	ndr	Encrypted	critical	OTHER	TLS_AES_256_GCM_SHA384	
5	10:47:37	FAIVMS0000000000	ndr	Encrypted	critical	OTHER	TLS_AES_256_GCM_SHA384	
6	10:47:32	FAIVMS0000000000	ndr	Weak cipher	high	OTHER	TLS_NULL_WITH_NULL_NULL	
7	10:47:32	FAIVMS0000000000	ndr	Encrypted	critical	OTHER	TLS_AES_256_GCM_SHA384	
8	10:47:32	FAIVMS0000000000	ndr	Encrypted	critical	OTHER	TLS_AES_256_GCM_SHA384	
9	10:47:27	FAIVMS0000000000	ndr	Encrypted	critical	OTHER	TLS_AES_256_GCM_SHA384	
10	10:47:22	FAIVMS0000000000	ndr	Encrypted	critical	OTHER	TLS_AES_256_GCM_SHA384	

This log type is supported in event handlers. In *FortiSoC > Handlers > Event Handler List*, you create event handlers with *Log Type = NDR Log (ndr)* when the *Log Device Type = FortiNDR*.



**Create New Handler**

Status: ☒ On

Name: FortiNDR - NDR log handler

Description:

Devices: ☒ All Devices ☐ Specify ☐ Local Device

Subnets: ☒ All Subnets ☐ Specify

Pre-filters: Add Pre-Filter

Filters: +

Filter 1: ☒ On

Log Device Type: FortiNDR

Log Type: NDR Log (ndr)

Group By: Source IP (srcip)

Logs match: ☐ All ☒ Any of the following conditions

In **FortiSoC > Event Monitor > All Events**, the events generated by this handler will display with **Event Type = ndr**.

#	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Handler
1	> [redacted] (37)	ndr	ndr	4438	Medium	18 hours ago	A minute ago	FNRD - NDR test
2	> [redacted] (37)	ndr	ndr	4430	Medium	18 hours ago	A minute ago	FNRD - NDR test
3	> [redacted] (37)	ndr	ndr	4434	Medium	18 hours ago	A minute ago	FNRD - NDR test
4	> reasons:N/A (37)	ndr	ndr	16872	Medium	18 hours ago	A minute ago	FNRD - NDR test
5	> [redacted] (37)	ndr	ndr	14513	Medium	18 hours ago	A minute ago	FNRD - NDR test
6	> Encrypted (37)	ndr	ndr	15157	Medium	18 hours ago	A minute ago	FNRD - NDR test
7	> ciphername:N/A (37)	ndr	ndr	15231	Medium	18 hours ago	A minute ago	FNRD - NDR test
8	> campaign:N/A (37)	ndr	ndr	16896	Medium	18 hours ago	A minute ago	FNRD - NDR test
9	> OTHER (39)	ndr	ndr	17305	Medium	18 hours ago	A minute ago	—
10	> critical (37)	ndr	ndr	15216	Medium	18 hours ago	A minute ago	FNRD - NDR test
11	> vname:N/A (37)	ndr	ndr	16813	Medium	18 hours ago	A minute ago	FNRD - NDR test

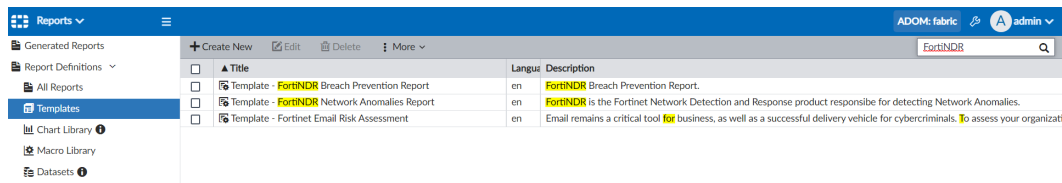
In **Reports > Report Definitions > Datasets**, new datasets are added for the FortiNDR device. These new datasets display in the table view with **Device Type = FortiNDR** and **Log Type = Vulnerability Scan**.

Name	Device Type	Log Type
fai-Files-Processed-Summary	FortiNDR	Event
fai-Host-quarantined-Summary	FortiNDR	Event
fai-Hosts-Infection-Summary	FortiNDR	Attack
fai-Leant-Customer-Features-Summary	FortiNDR	Event
fai-Malicious-File-Summary	FortiNDR	Attack
fai-Malware-Detection-Type-Summary	FortiNDR	Attack
fai-System-Events-Summary	FortiNDR	Event
fndr-Anomaly-Count-by-Severity	FortiNDR	Vulnerability Scan
fndr-Anomaly-Count-by-Severity-Timeline	FortiNDR	Vulnerability Scan
fndr-Anomaly-Type-and-Feature-by-Count	FortiNDR	Vulnerability Scan
fndr-Botnet-Name-by-Count	FortiNDR	Vulnerability Scan
fndr-Botnet-Severity-by-Count	FortiNDR	Vulnerability Scan
fndr-Botnet-Traffic-Summary	FortiNDR	Vulnerability Scan
fndr-Encrypted-Attack-Summary	FortiNDR	Vulnerability Scan
fndr-Encrypted-Severity-by-Count	FortiNDR	Vulnerability Scan

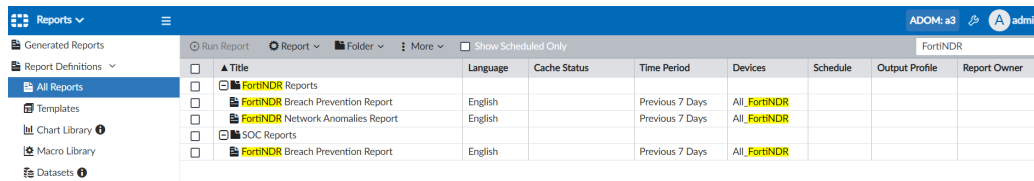
In **Reports > Report Definitions > Macro Library**, new macros are added for the FortiNDR device. These new macros display in the table view with **Device Type = FortiNDR** and **Category = Vulnerability Scan**.

Name	Description	Device Type	Category
FortiNDR: FortiSandbox Files Accepted	FortiSandbox Files Accepted	FortiNDR	Event
FortiNDR: FortiSandbox Files Detected	FortiSandbox Files Detected	FortiNDR	Event
FortiNDR: FortiSandbox Files Processed	FortiSandbox Files Processed	FortiNDR	Event
FortiNDR: Total Number of Critical Anomalies	FortiNDR: Total Number of Critical Anomalies	FortiNDR	Vulnerability Scan
FortiNDR: Total Number of High Anomalies	FortiNDR: Total Number of High Anomalies	FortiNDR	Vulnerability Scan
FortiNDR: Total Number of Low Anomalies	FortiNDR: Total Number of Low Anomalies	FortiNDR	Vulnerability Scan
FortiNDR: Total Number of Medium Anomalies	FortiNDR: Total Number of Medium Anomalies	FortiNDR	Vulnerability Scan

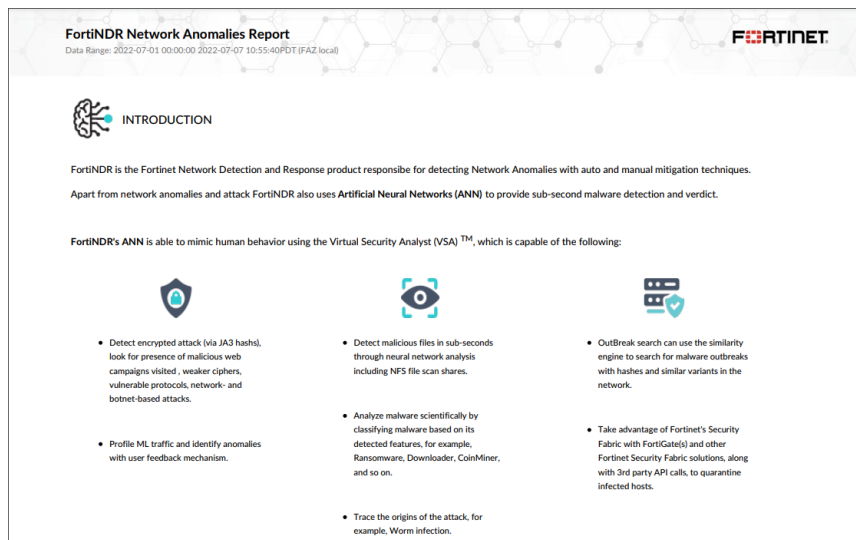
In **Reports > Report Definitions > Templates**, a new default report template is added: **Template - FortiNDR Network Anomalies Report**.



This template can be used to create a report. You can also use the default report in *Reports > Report Definitions > All Reports*.



Below is a sample of the *FortiNDR Network Anomalies Report* in PDF format.



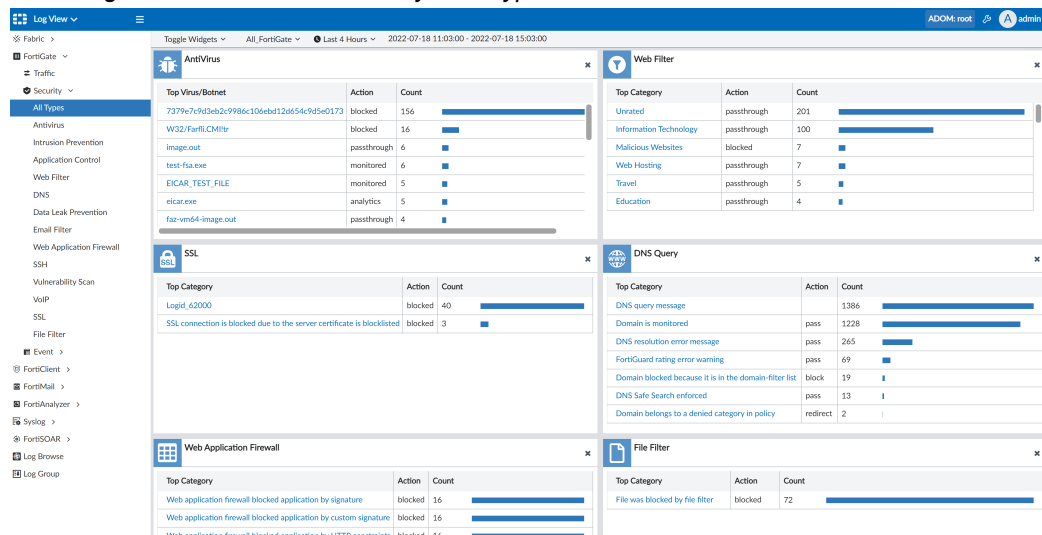
## Security events consolidated page - 7.2.1

Security logs are consolidated in a new widget style page: *Log View > FortiGate > Security > All Types*.

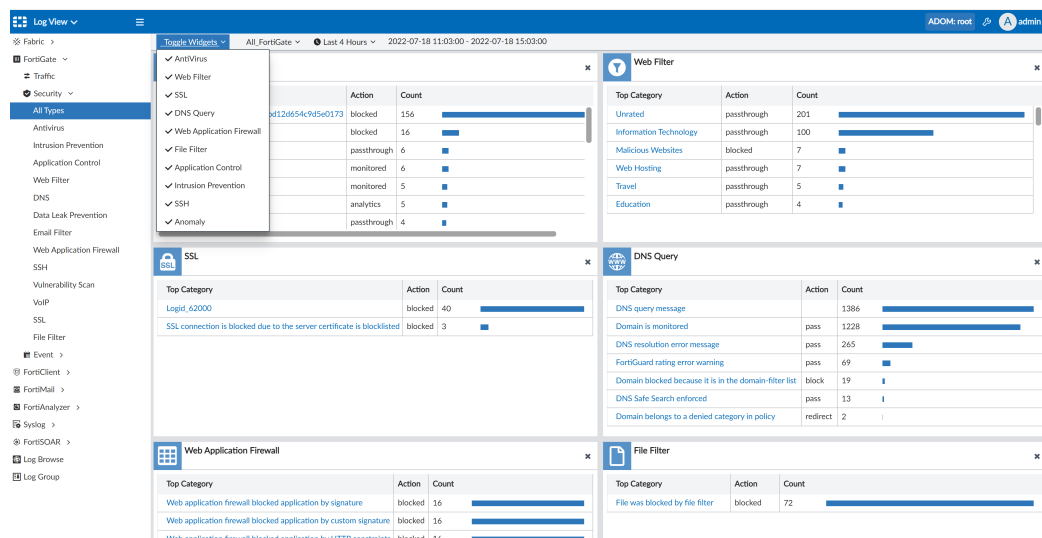
To simplify monitoring, security log subtypes such as *AntiVirus* and *Web Filter* are presented in individual widgets. Each widget lists the most frequent events by count in descending order. By clicking any consolidated entry, you can drill-down to the exact log entries.

## To view the security logs dashboard:

### 1. Go to *Log View > FortiGate > Security > All Types*.



### 2. From the *Toggle Widgets* dropdown, select the widgets to display on the dashboard. You can also toggle widgets off by clicking **X** on the widget.



### 3. Click an entry in the following widgets to display the details in the security view.

- *AntiVirus*
- *Web Filter*
- *Web Application Firewall*
- *Application Control*
- *Intrusion Prevention*
- *Anomaly*

See the example below that drills down from the *AntiVirus* widget.

The screenshot displays the FortiAnalyzer Log View interface. The left sidebar shows the navigation menu with 'Log View' selected. The main area contains several widgets:

- AntiVirus:** Shows a table of virus/botnet detections. The entry 'EICAR\_TEST\_FILE' is highlighted in blue.
- Web Filter:** Shows a table of web filter actions. The entry 'Unrated' is highlighted in blue.
- SSL:** Shows a table of SSL connections. The entry 'SSL connection is blocked due to the server certificate is blocklisted' is highlighted in blue.
- DNS Query:** Shows a table of DNS query actions. The entry 'DNS query message' is highlighted in blue.
- Web Application Firewall:** Shows a table of WAF actions. The entry 'Web application firewall blocked application by HTTP constraints' is highlighted in blue.
- File Filter:** Shows a table of file filter actions. The entry 'File was blocked by file filter' is highlighted in blue.

Below the widgets, a table shows the log entries for the selected event. The table has columns: #, Date/Time, Device ID, Action, Source, Service, Destination IP, Virus/Botnet, User, and File Name. The entry 'EICAR\_TEST\_FILE' is highlighted in blue.

4. Click an entry in the following widgets to display the event view filtered by the Log ID for details.

- *DNS Query*
- *File Filter*
- *SSH*
- *SSL*

See the example below that drills down from the *SSH* widget.

The screenshot displays the FortiAnalyzer Log View interface with the 'SSH' widget selected. The left sidebar shows the navigation menu with 'SSH' selected. The main area contains several widgets:

- Web Application Firewall:** Shows a table of WAF actions. The entry 'Web application firewall blocked application by signature' is highlighted in blue.
- Application Control:** Shows a table of application control actions. The entry 'Network.Service' is highlighted in blue.
- Intrusion Prevention:** Shows a table of intrusion prevention actions. The entry 'UDPPORT0' is highlighted in blue.
- SSH:** Shows a table of SSH actions. The entry 'SSH channel is blocked' is highlighted in blue.
- Anomaly:** Shows a table of anomaly actions. The entry 'tcp\_syn\_flood' is highlighted in blue.

Below the widgets, a table shows the log entries for the selected event. The table has columns: #, Date/Time, Device ID, Action, Source, Service, Destination IP, Virus/Botnet, User, and File Name. The entry 'SSH channel is blocked' is highlighted in blue.

The screenshot displays the FortiAnalyzer Log View interface. The left sidebar shows a navigation menu with categories like Fabric, FortiGate, Traffic, Security, and various security modules. The main pane shows a table of logs filtered by 'Action = blocked' and 'Log ID = 61010'. The table columns are #, Date/Time, Sub Type, Action, Source, Profile, Direction, and Login. All entries show 'blocked' actions for 'ssh' sub-type, originating from 'user4' or 'user (1.1.1.1)' and going to 'ssh-log-test-login' via 'ssh-log-test-filter' in an 'outgoing' direction. The bottom status bar indicates 'Total logs for analytics: 21 days 3 hours' and '1000 Items per page'.

#	Date/Time	Sub Type	Action	Source	Profile	Direction	Login
1	15:02:33	ssh	blocked	user4	ssh-log-test-filter	outgoing	ssh-log-test-login
2	15:02:32	ssh	blocked	user4	ssh-log-test-filter	outgoing	ssh-log-test-login
3	15:02:31	ssh	blocked	user4	ssh-log-test-filter	outgoing	ssh-log-test-login
4	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
5	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
6	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
7	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
8	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
9	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
10	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
11	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
12	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
13	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
14	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
15	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
16	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
17	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
18	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
19	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
20	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
21	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
22	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
23	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
24	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
25	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
26	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
27	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
28	14:55:46	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
29	14:41:08	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
30	14:41:08	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login
31	14:41:08	ssh	blocked	user (1.1.1.1)	ssh-log-test-filter	outgoing	ssh-log-test-login

## Reports

This section lists the new features added to FortiAnalyzer for reports:

- [Report in JSON format on page 69](#)
- [Report cache control on page 70](#)
- [Upgrade report editor on page 71](#)
- [Improve data visualization for the web usage report on page 74](#)
- [360 Security Report on page 76](#)
- [VPN report update 7.2.1 on page 78](#)
- [Application risk and control report update 7.2.1 on page 82](#)
- [Bandwidth and applications report update 7.2.1 on page 84](#)
- [Security events and incidents summary report update 7.2.1 on page 85](#)
- [High bandwidth application usage report update 7.2.1 on page 87](#)
- [Cyber-bullying indicators report update 7.2.1 on page 89](#)
- [Self-harm and risk indicators report update 7.2.2 on page 91](#)

## Report in JSON format

The JSON format is now available for reports.

### To download a report in the JSON format:

1. After running the report, go to *Reports > Generated Reports*.
2. In the *Format* column for the report, click *JSON*.

Report Name	Format	Time Range	Devices	Status
360-Degree Security Review-2022-02-18-1052_877	HTML PDF XML CSV JSON	2022/02/11 - 2022/02/17	11 Devices (including 11 VDOMs) >	34s
▼ Earlier This Week (136)				
Cyber Threat Assessment-2022-02-17-1534_875	HTML PDF XML CSV JSON	2022/02/10 - 2022/02/16	6 Devices (including 6 VDOMs) >	20s
Client Reputation-2022-02-17-1534_873	HTML PDF XML CSV JSON	2022/02/10 - 2022/02/16	11 Devices (including 11 VDOMs) >	3s
Client Reputation-2022-02-17-1530_871	HTML PDF XML CSV JSON	2022/02/10 - 2022/02/16	11 Devices (including 11 VDOMs) >	4s
Client Reputation-2022-02-17-1530_869	HTML PDF XML CSV JSON	2022/02/10 - 2022/02/16	11 Devices (including 11 VDOMs) >	4s
Client Reputation-2022-02-17-1505_867	HTML PDF XML CSV JSON	2022/02/10 - 2022/02/16	11 Devices (including 11 VDOMs) >	4s
Client Reputation-2022-02-17-1505_865	HTML PDF XML CSV JSON	2022/02/10 - 2022/02/16	11 Devices (including 11 VDOMs) >	4s
Cyber Threat Assessment-2022-02-17-1504_862	HTML PDF XML CSV JSON	2022/02/10 - 2022/02/16	6 Devices (including 6 VDOMs) >	21s
Cyber Threat Assessment-2022-02-17-1504_861	HTML PDF XML CSV JSON	2022/02/10 - 2022/02/16	6 Devices (including 6 VDOMs) >	21s
Client Reputation-2022-02-17-1500_859	HTML PDF XML CSV JSON	2022/02/10 - 2022/02/16	11 Devices (including 11 VDOMs) >	4s

## Report cache control

Admins can now control caching for individual reports in the report settings.

### To control the report cache for an individual report:

1. Go to *Reports > All Reports*, and double-click the report to edit.
2. Go to the *Settings* tab.
3. Expand the *Advanced Settings* for the report.
4. Configure the following options to control the report cache:

#### Enable Report Filter Caching

Select to accelerate processing speed when generating multiple reports. In this case, all filters are applied when querying the hcache table. This is the default.

De-select to improve report accuracy. In this case, the filters are put inside the hcache to increase data accuracy. However, this will also impact performance.

#### Enable High Accuracy Caching

Select to increase the maximum hcache rows, increasing data accuracy.

You can show, set, or reset the maximum number of rows for high-accuracy hcache by entering the following command in the FortiAnalyzer CLI:

```
diagnose sql config hcache-max-high-accu-row [reset | set <integer>]
```

De-select to use the default number of hcache rows, increasing system performance. This is the default.

You can show, set, or reset the default number of hcache rows by entering the following command in the FortiAnalyzer CLI:

```
diagnose sql config hcache-max-rpt-row [reset | set <integer>]
```

5. Click *Apply* to save the changes.

Reports ▾

Security Fabric Demo 1 Admin1 ▾

Generated Reports

Report Definitions ▾

All Reports

Templates

Chart Library ⓘ

Macro Library

Datasets ⓘ

Advanced ▾

Language

Output Profile

Report Calendar

Edit: 360-Degree Security Review

Generated Reports Settings Editor

Advanced Settings ▾

Language English ▾

Bundle Rest into "Others" Auto ▾

Print Orientation ☒ Portrait ☐ Landscape

Chart Heading Level Heading 2 ▾

Default Font Open Sans ▾

☒ Hide # Column

☒ Layout Header

Header Text

Header Image Select Image fortinet\_grey.png

☒ Layout Footer

☒ Print Cover Page

☒ Print Table of Contents

☒ Print Device List Compact ▾

☒ Print Report Filters

☐ Obfuscate User

☐ Resolve Hostname

Date Format Default ▾

Allow save maximum 99

Color Code Blue ▾

Report Owner Click to select ▾

☒ Enable Report Filter Caching

☐ Enable High Accuracy Caching

Apply Return

## Upgrade report editor

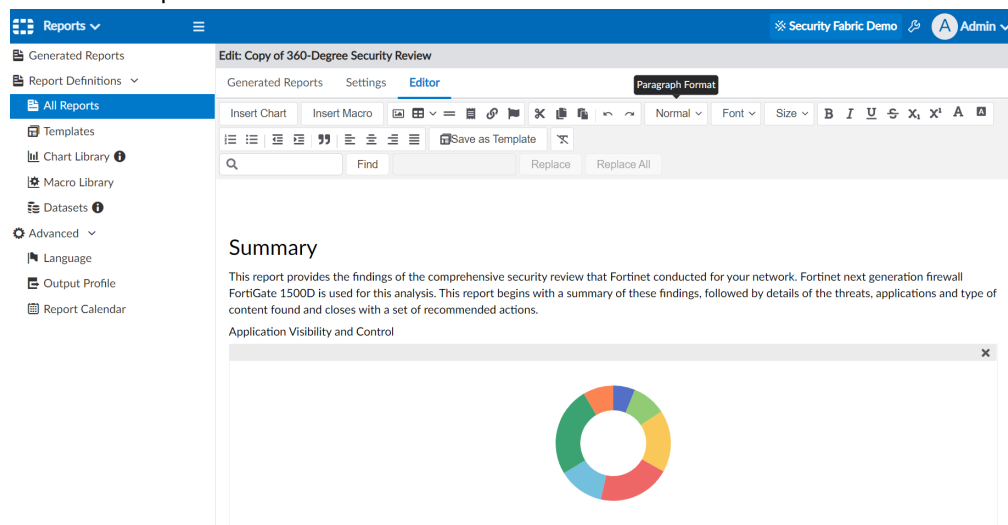
The report editor has been replaced with a custom rich text editor.

### To use the report editor:

1. Go to *Reports > Report Definitions > All Reports*.
2. Right click a report and select *Edit*.
3. Go to the *Editor* tab.

The *Editor* tab is also available when creating a new report.

#### 4. Mouse over options in the toolbar to view the related action.



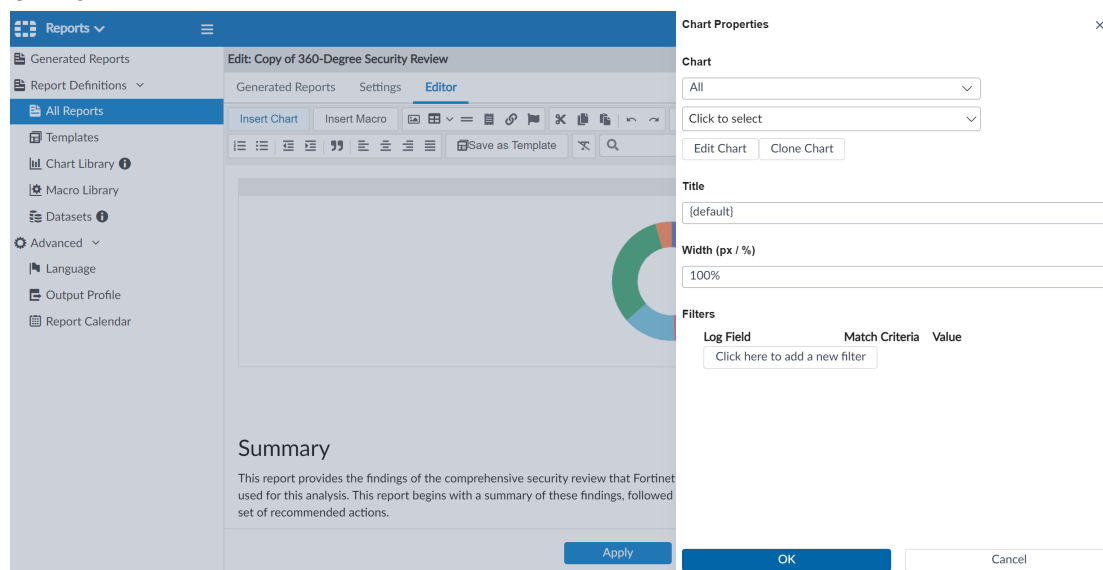
You can also use the following shortcuts in the editor:

- **CTRL+C** to copy text
- **CTRL+X** to cut text
- **CTRL+V** to paste copied or cut text
- **CTRL+Z** to undo
- **CTRL+Y** to redo
- **CTRL+B** to apply bold formatting
- **CTRL+I** to apply italic formatting
- **CTRL+U** to apply underline formatting

#### 5. To add a chart in the report, click *Insert Chart*.

#### 6. In the *Chart Properties* pane, select a chart, enter a title, adjust the width, and set the filters.

#### 7. Click *OK*.

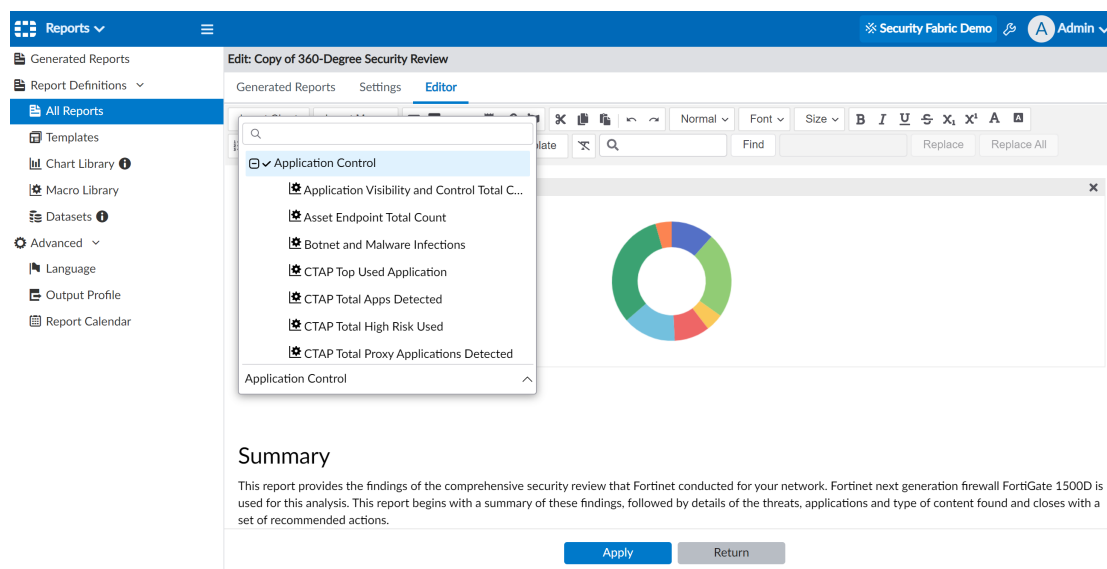


#### 8. To add a macro in the report, click *Insert Macro*.

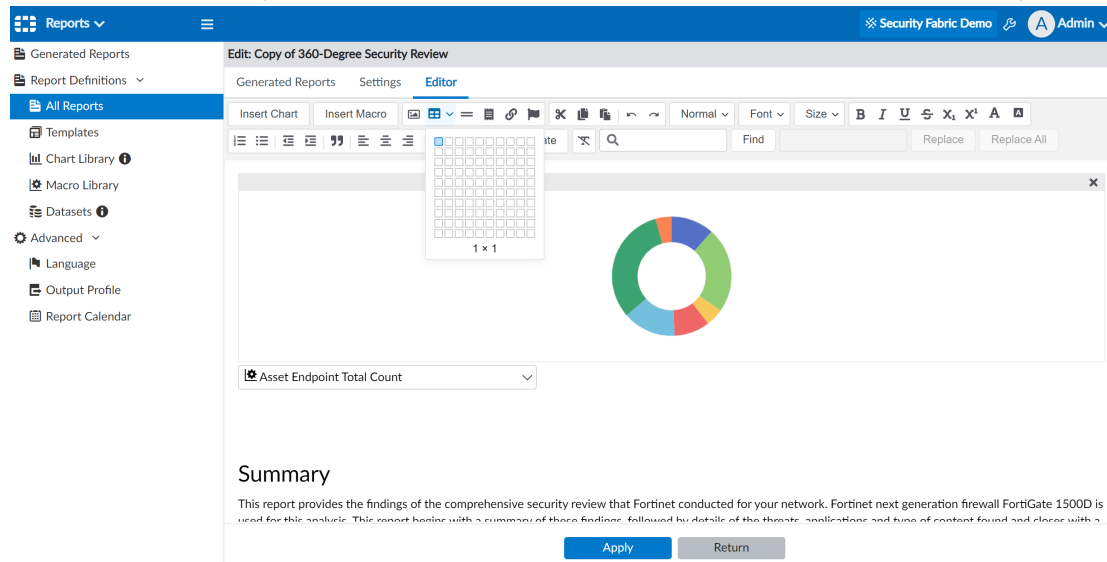
#### 9. From the macro dropdown in the report, select a macro.

You can delete the macro as though it is regular text by using the backspace key.

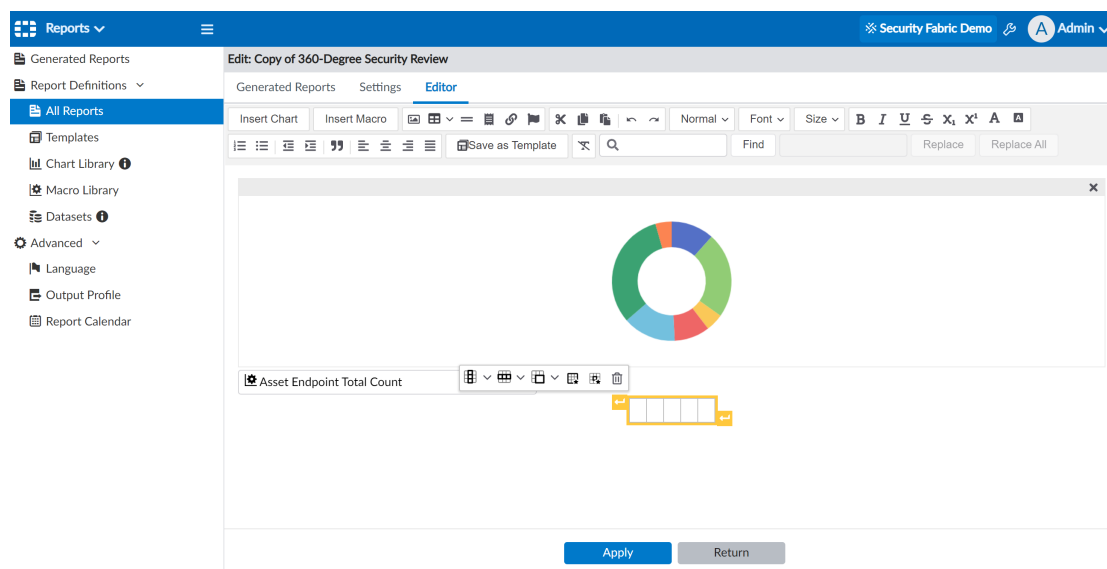




10. To add a table in the report, select the number of rows and columns from the insert table dropdown.



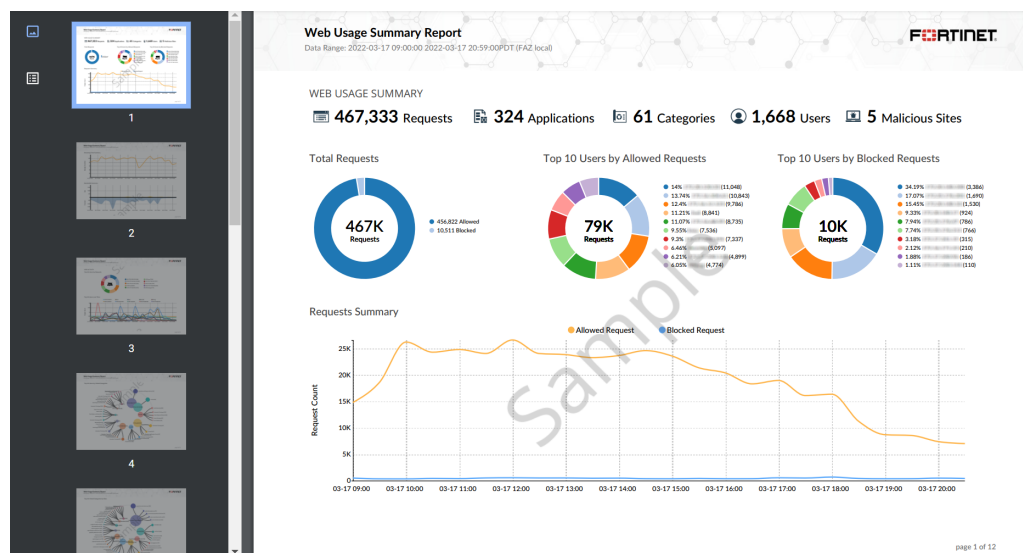
11. Click the table to use icons for editing the table.  
You can use the yellow arrows at the edge to add space above or below the selected chart or table.

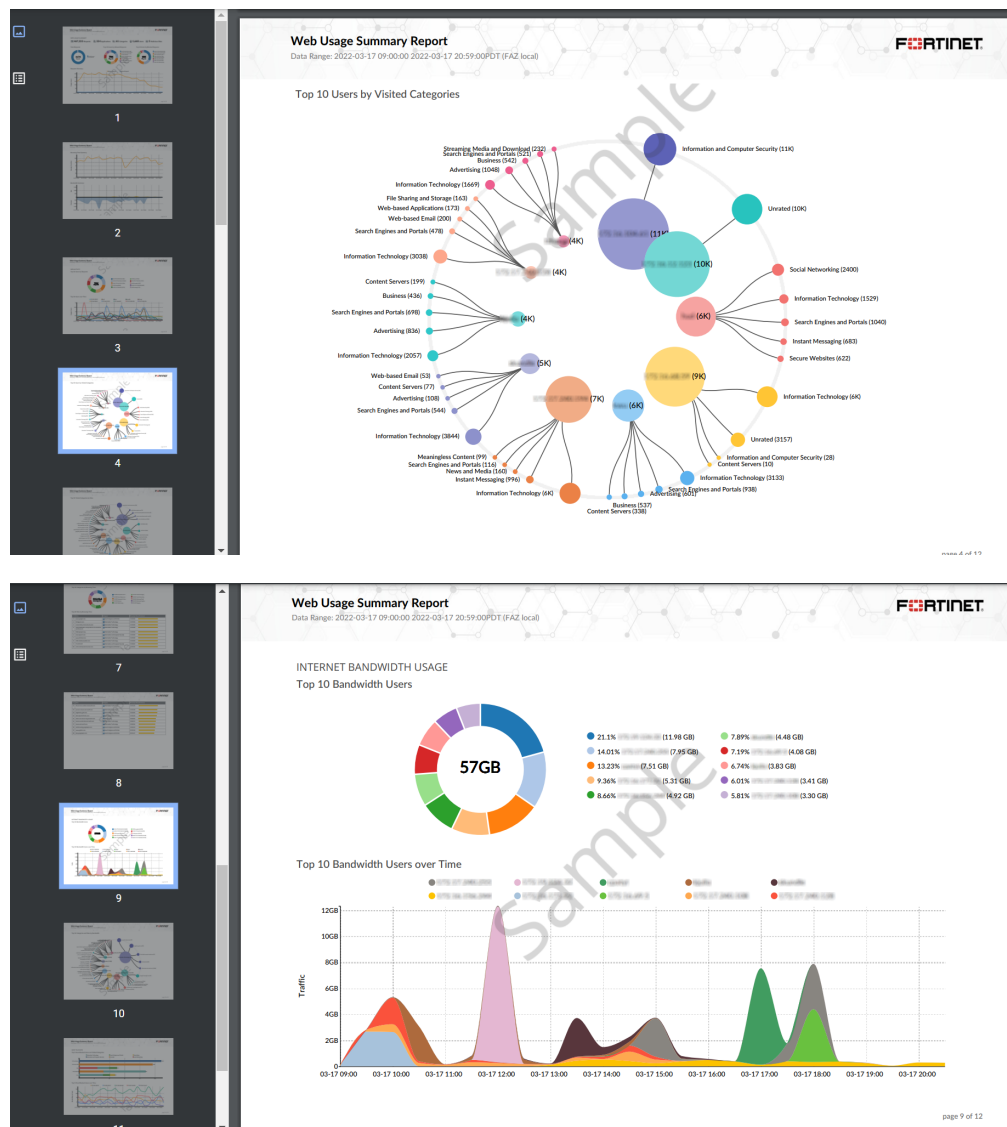


## Improve data visualization for the web usage report

A new *Web Usage Summary Report* is implemented based on the existing *Web Usage Report*. This report provides an enhanced user experience with improved charts and graphs.

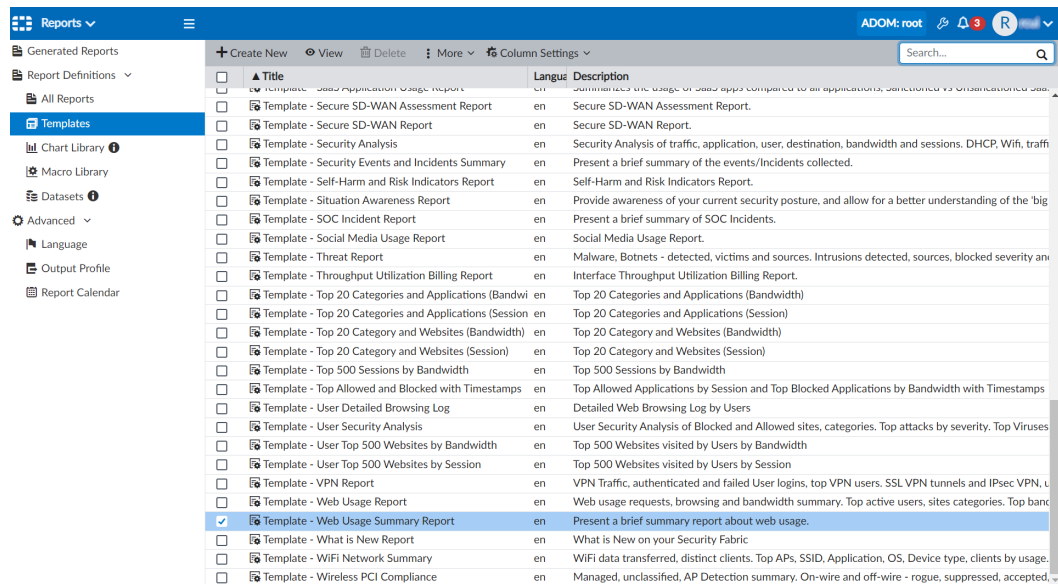
For example, below is a sample of the report in PDF format.





### To use the Web Usage Summary Report template:

1. Go to *Reports > Report Definitions > Templates*.  
From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Web Usage Summary Report*.
3. From the *More* dropdown, click *Clone* to clone template and make adjustments.  
You can also click *Create Report* to create a report using the template.



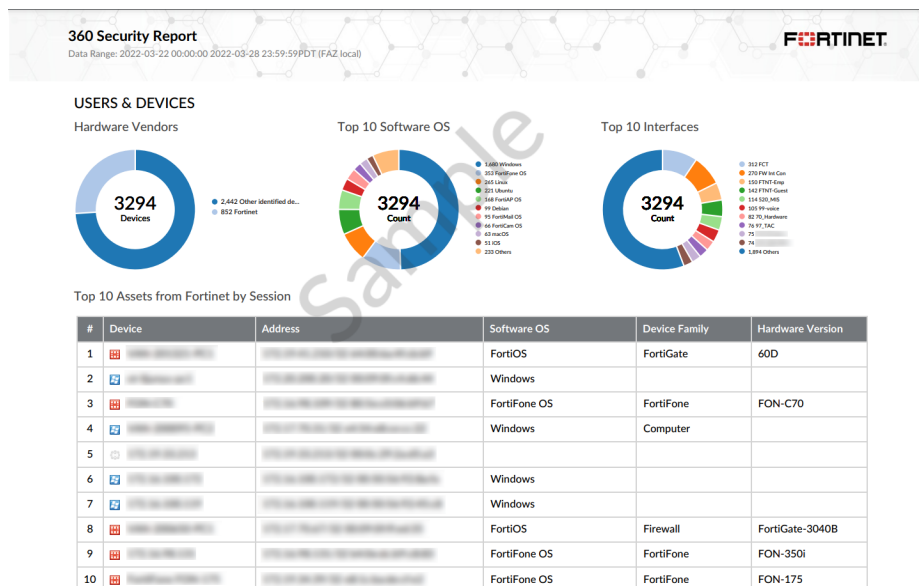
### To run the web usage report:

1. Go to **Reports > All Reports**, and double-click the row for **Web Usage Summary Report**. The **Edit: Web Usage Summary Report** pane opens.
2. Click **Run Report**.
3. Once the report is available, click the format to view the report in.

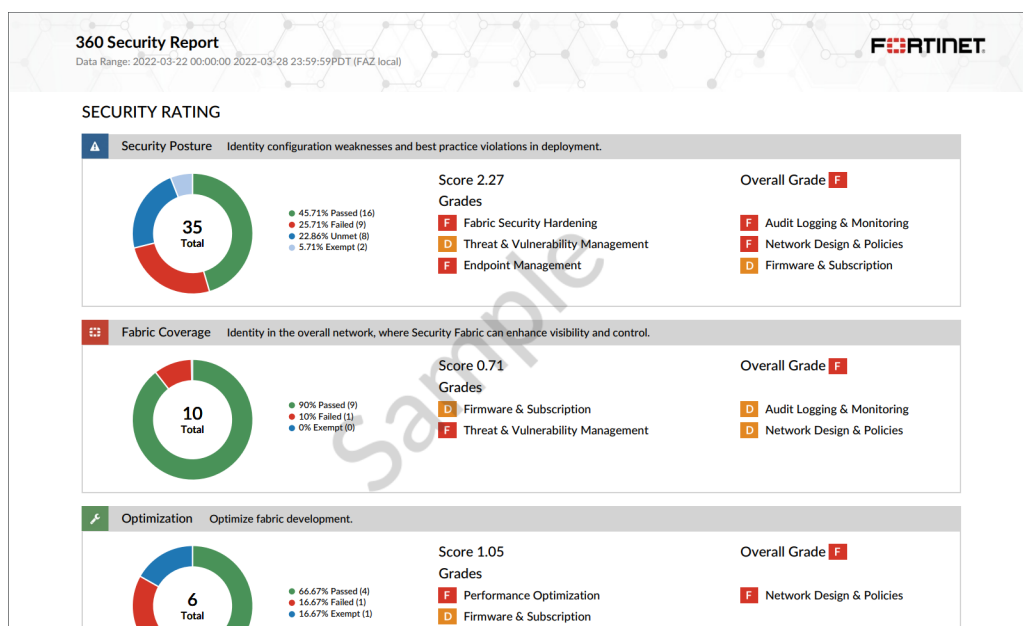
## 360 Security Report

A new **360 Security Report** is implemented based on the existing **360-Degree Security Review Report**.

The **360 Security Report** includes data from the FortiOS security rating, providing an enhanced user experience with organized charts and graphs. For example, see a sample of the report in PDF format below.



page 1 of 21



### To use the 360 Security Report template:

- Go to *Reports > Report Definitions > Templates*.  
From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
- Select the checkbox for *Template - 360 Security Report*.
- From the *More* dropdown, click *Clone* to clone template and make adjustments.  
You can also click *Create Report* to create a report using the template.

Reports		ADOM: root		admin	
Generated Reports	+ Create New View Delete More			Search...	
Report Definitions					
All Reports					
Templates	<input type="checkbox"/>	Title		Category	Preview
Chart Library	<input type="checkbox"/>	Template - 360 Protection Report	ware inventory of the FortiGate devices over a 30 day period.	System	HTML PDF
Macro Library	<input checked="" type="checkbox"/>	Template - 360 Security Report	ic, threat, app, user, incident, compromised host and so on.	Security	HTML PDF
Datasets	<input type="checkbox"/>	Template - 360-Degree Security Review	d Control, Threat Detection, Data Exfiltration Detection, Endpoint Detection, P	Security	HTML PDF
Advanced	<input type="checkbox"/>	Template - Admin and System Events Report	system severity event counts.	System	HTML PDF
	<input type="checkbox"/>	Template - Application Risk and Control	app, web categories, vulnerability exploits, virus, botnet, adware malicious attac	Application	HTML PDF
	<input type="checkbox"/>	Template - Asset and Identity Report	and their users, vulnerabilities, software installed as well as running processes.	Assets	HTML PDF
	<input type="checkbox"/>	Template - Bandwidth and Applications Repo	summaries - by users and applications	Application	HTML PDF

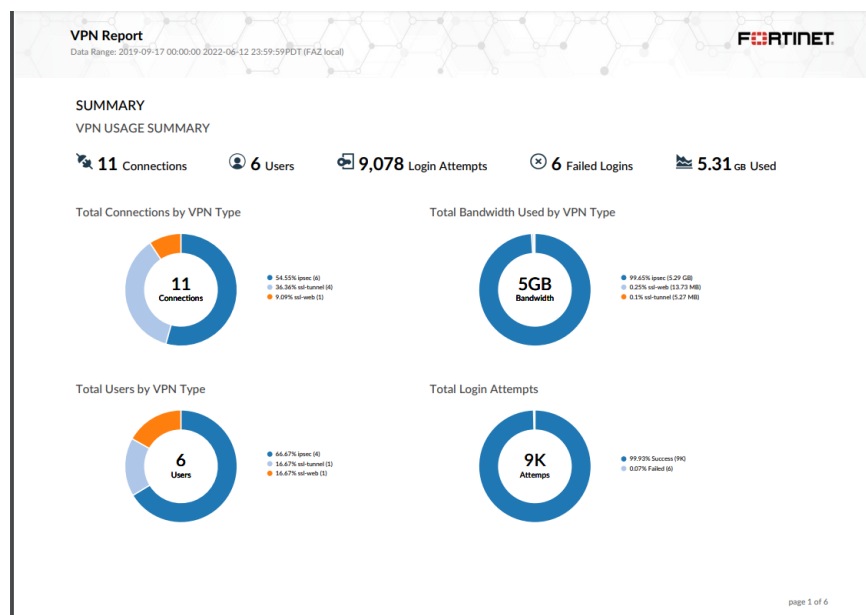
### To run the 360 Security Report:

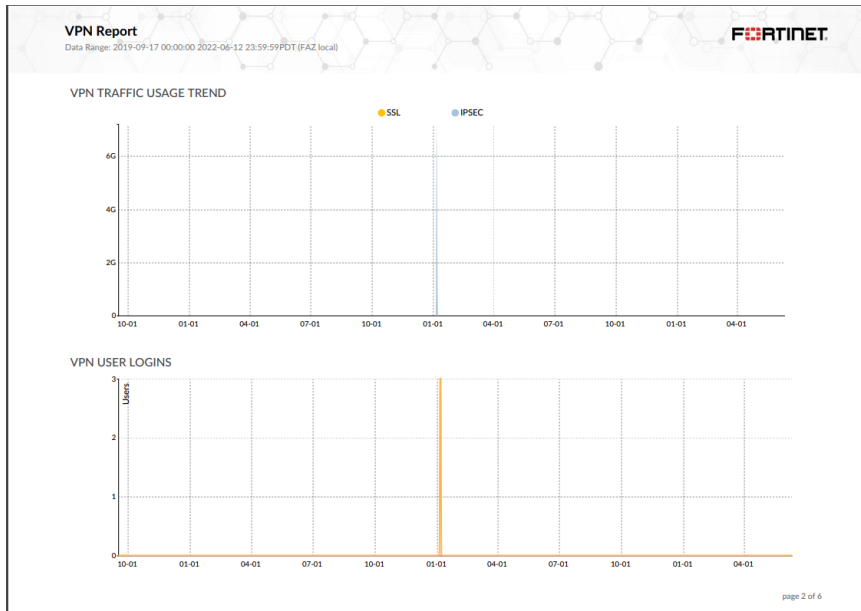
1. Go to *Reports > All Reports*, and double-click the row for *360 Security Report*. The *Edit: 360 Security Report* pane opens.
2. Click *Run Report*.
3. Once the report is available, click the format to view the report in.

## VPN report update - 7.2.1

The VPN report has been updated with a new visualization, more analytics, and better organization.

For example, below is a sample of the report in PDF format.





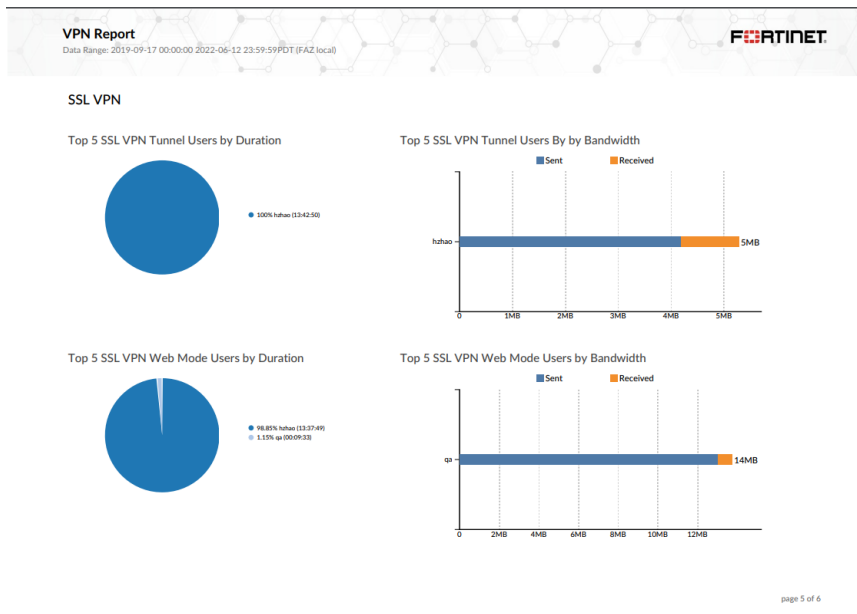
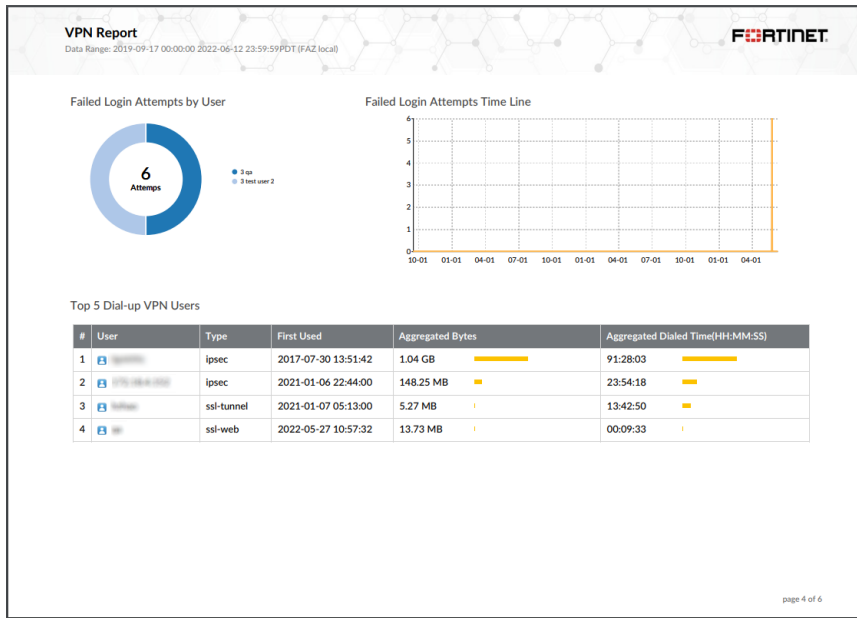
**VPN Report**  
Data Range: 2019-09-17 00:00:00 2022-06-12 23:59:59 PDT (FAZ local)

**AUTHENTICATED LOGINS**

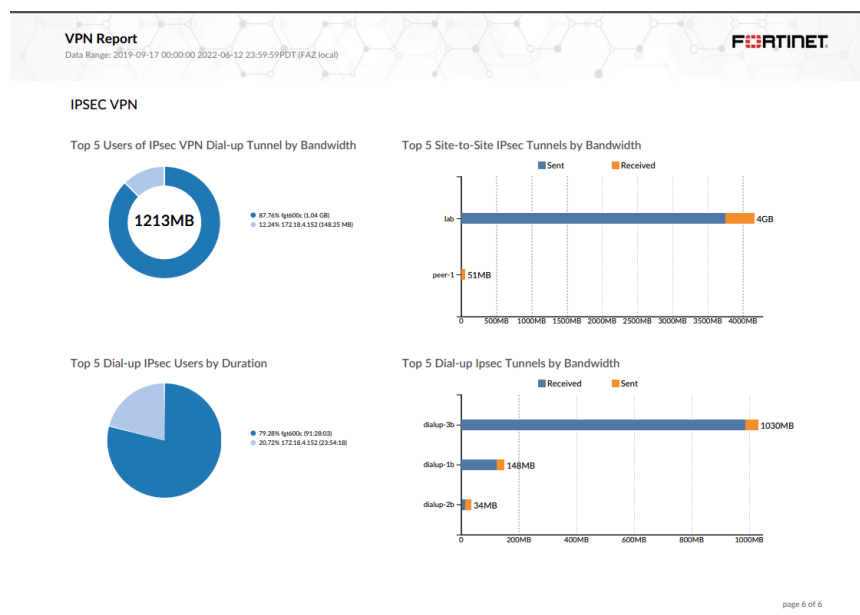
Top 15 Authenticated Logins by VPN Connections

#	User	Type	First Used	Total Number of Connections	Total Duration Connected(HH-MM-SS)
1	admin	ssl-tunnel	2021-01-07 05:13:00	4	13:42:50
2	ipsec@fa	ipsec	2017-07-30 13:51:42	3	91:28:03
3	172.16.4.128	ipsec	2020-03-15 12:22:01	1	46:40:03
4	172.16.4.128	ipsec	2021-01-06 22:44:00	1	23:54:18
5	172.16.4.128	ipsec	2021-01-06 22:44:00	1	23:54:18
6	ip	ssl-web	2022-05-27 10:57:32	1	00:09:33

page 3 of 6







### To use the VPN Report template:

1. Go to *Reports > Report Definitions > Templates*.  
From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - VPN Report*.
3. From the *More* dropdown, click *Clone* to clone the template and make adjustments.  
You can also click *Create Report* to create a report using the template.

Reports

Generated Reports

Report Definitions

All Reports

Templates

Chart Library

Macro Library

Datasets

Advanced

Language

Output Profile

Report Calendar

Create New

View

Delete

More

Search...

Title

Template - Top 20 Category and Websites (Session)

Template - Top 500 Sessions by Bandwidth

Template - Top Allowed and Blocked Applications by Session

Template - User Detailed Browsing Log

Template - User Security Analysis

Template - User Top 500 Websites by Bandwidth

Template - User Top 500 Websites by Session

Template - VPN Report

Template - Web Usage Report

Template - Web Usage Summary Report

Template - What is New Report

Template - WiFi Network Summary

Template - Wireless PCI Compliance

Clone

Create Report

Install Template Pack

Language

en

en

en

en

en

en

en

en

en

en

en

en

en

en

Description

Top 20 Category and Websites (Session)

Top 500 Sessions by Bandwidth

Top Allowed Applications by Session

Detailed Web Browsing Log by Users

User Security Analysis of Blocked and Allowed Applications

Top 500 Websites visited by Users by Bandwidth

Top 500 Websites visited by Users by Session

VPN Traffic, authenticated and failed

Web usage requests, browsing and blocked

Present a brief summary report about web usage

What is New on your Security Fabric

WiFi data transferred, distinct clients, and SSIDs

Managed, unclassified, AP Detection and Mitigation

Category

Web

Web

Application

User

User

User

User

Security

Security

Security

Security

Security

Security

Security

Preview

HTML PDF

HTML PDF

HTML PDF

HTML PDF

HTML PDF

HTML PDF

HTML PDF

HTML PDF

HTML PDF

HTML PDF

HTML PDF

HTML PDF

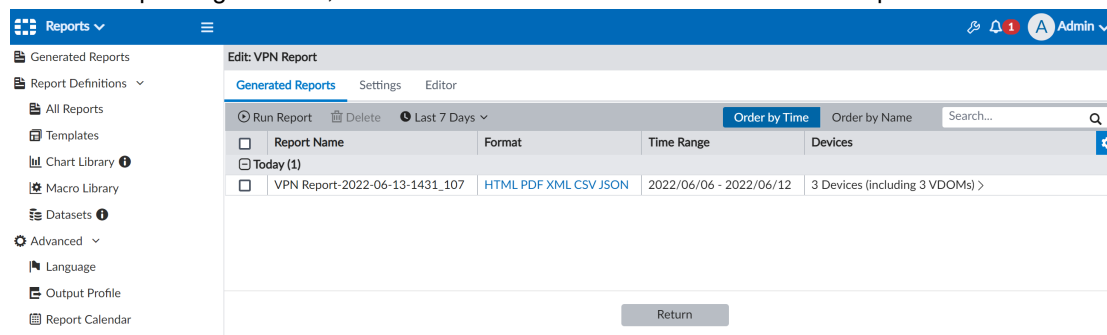
HTML PDF

HTML PDF

### To run the VPN Report:

1. Go to *Reports > Report Definitions > All Reports*.
2. Double-click the row for *VPN Report*.
3. In the *Generated Reports* tab, click *Run Report*.

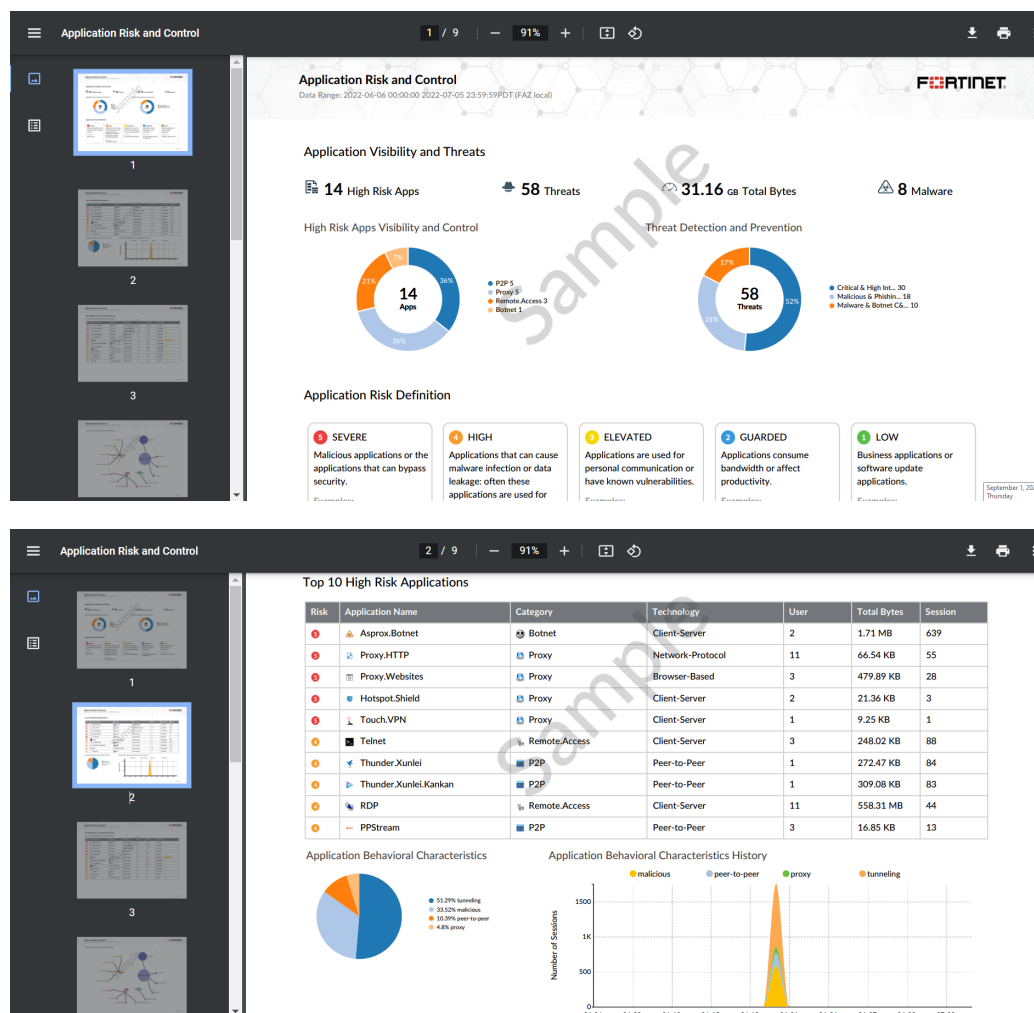
4. Once the report is generated, click a format in the *Format* column to view the report.

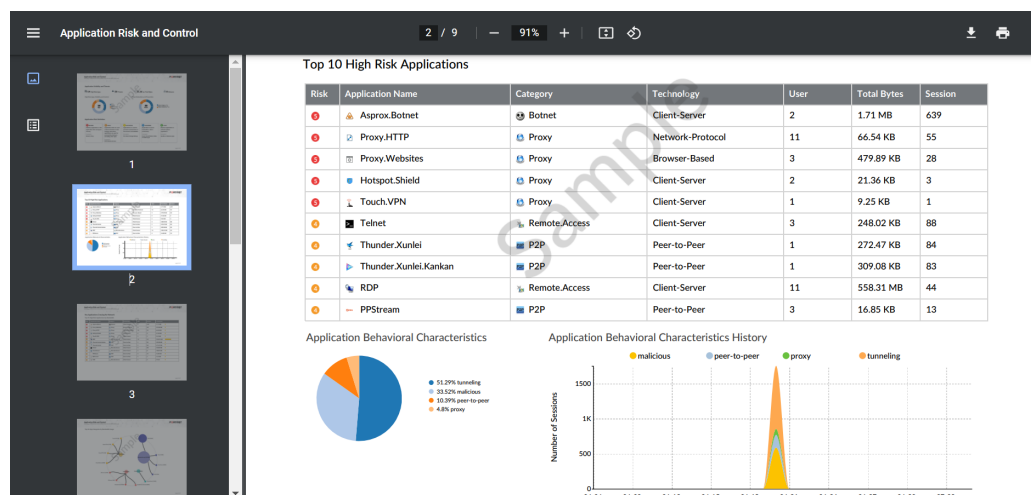


## Application risk and control report update - 7.2.1

The *Application Risk and Control* report is updated to improve data visualization.

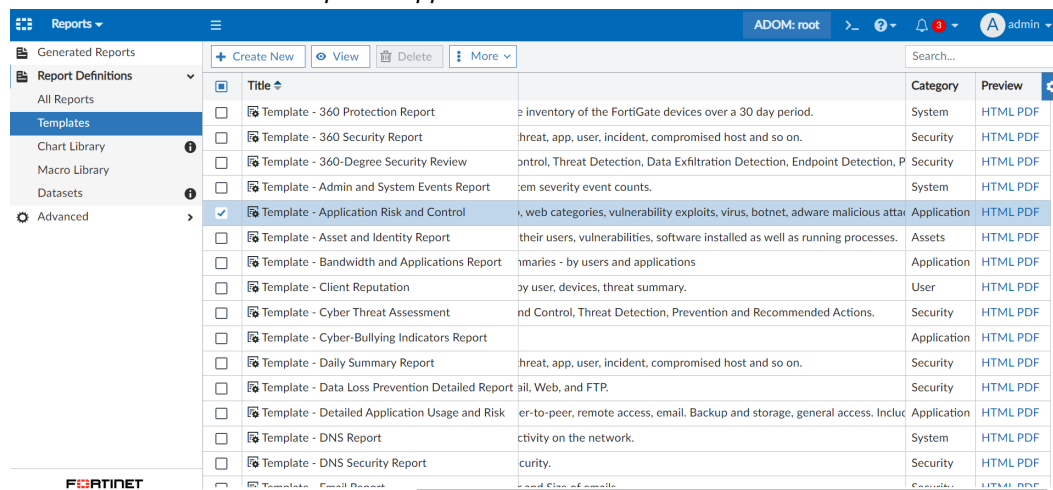
For example, below is a sample of the report in PDF format.





### To use the Application Risk and Control report template:

- Go to **Reports > Report Definitions > Templates**.  
From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
- Select the checkbox for *Template - Application Risk and Control*.



- From the *More* dropdown, click *Clone* to clone the template and make adjustments.  
You can also click *Create Report* to create a report using the template.

### To run the Application Risk and Control report:

- Go to **Reports > Report Definitions > All Reports**.
- Double-click the row for *Application Risk and Control*.  
You can find the report using the search bar. For example, see the image below.

Reports									
Generated Reports	Run Report	Report	Folder	More	Show Scheduled Only	application risk			
Report Definitions									
All Reports									
Templates									
Chart Library									
Macro Library									
Datasets									
Advanced									

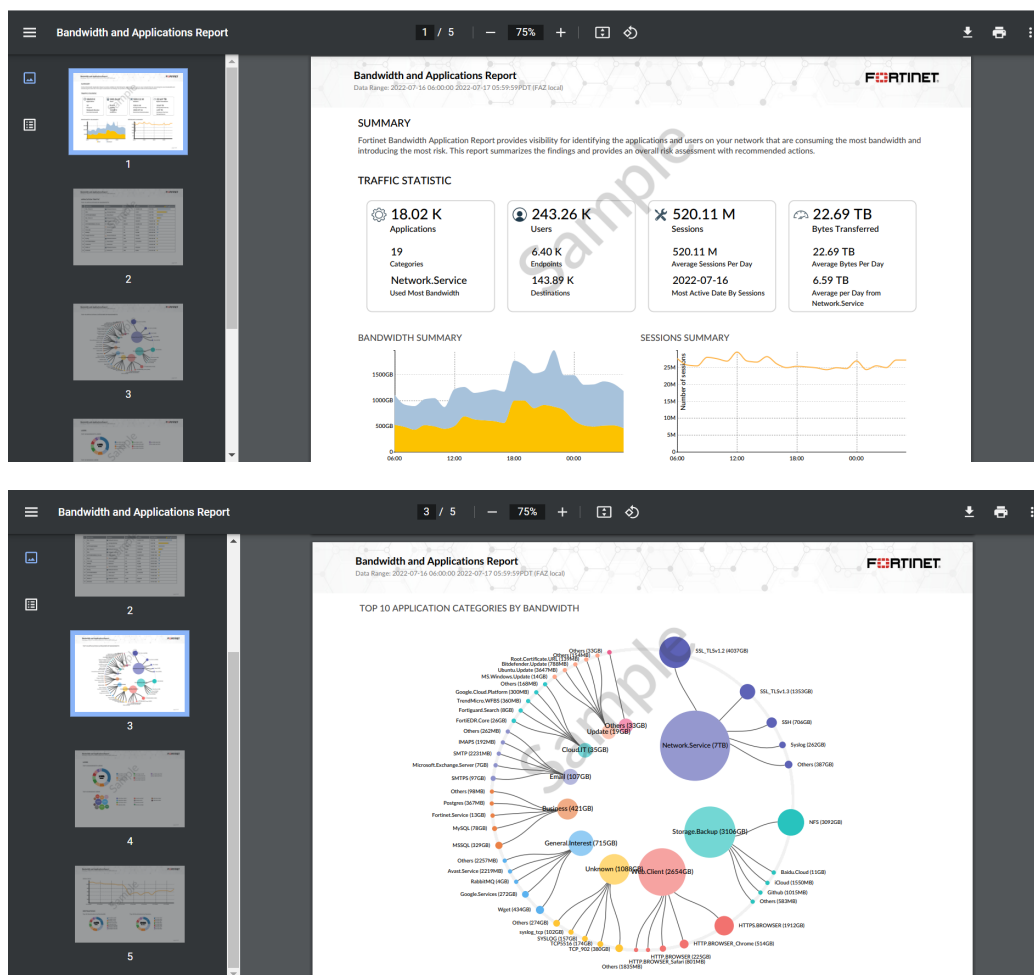
Title	Language	Cache Status	Time Period	Devices	Schedule	Output Profile	Report Own
Application Reports							
Application Risk and Control	English		Previous 7 Days	All_FortiGate			
FortiGate Reports							
Application Risk and Control	English		Previous 7 Days	All_FortiGate			
SOC Reports							
Application Risk and Control	English		Previous 7 Days	All_FortiGate			

3. In the *Generated Reports* tab, click *Run Report*.
4. Once the report is generated, click a format in the *Format* column to view the report.

## Bandwidth and applications report update - 7.2.1

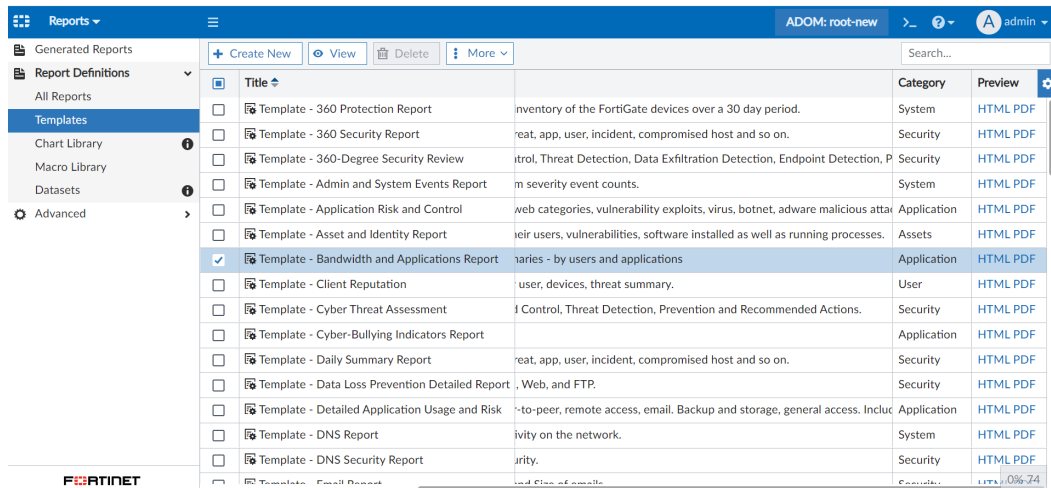
The *Bandwidth and Applications Report* is updated to improve data visualization.

For example, below is a sample of the report in PDF format.



### To use the Bandwidth and Applications Report template:

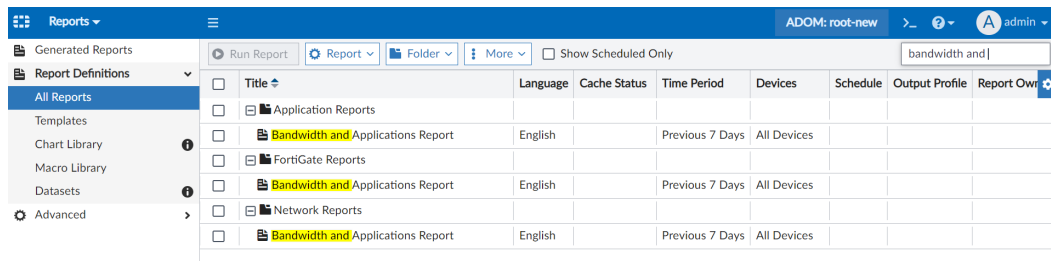
1. Go to *Reports > Report Definitions > Templates*.  
From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Bandwidth and Applications Report*.



3. From the *More* dropdown, click *Clone* to clone the template and make adjustments.  
You can also click *Create Report* to create a report using the template.

### To run the Bandwidth and Applications Report:

1. Go to *Reports > Report Definitions > All Reports*.
2. Double-click the row for *Bandwidth and Applications Report*.  
You can find the report using the search bar. For example, see the image below.

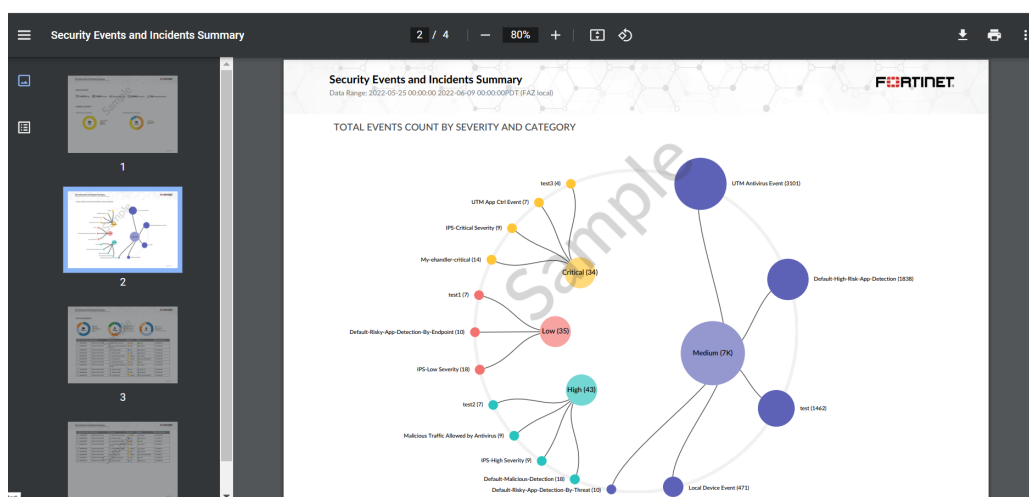
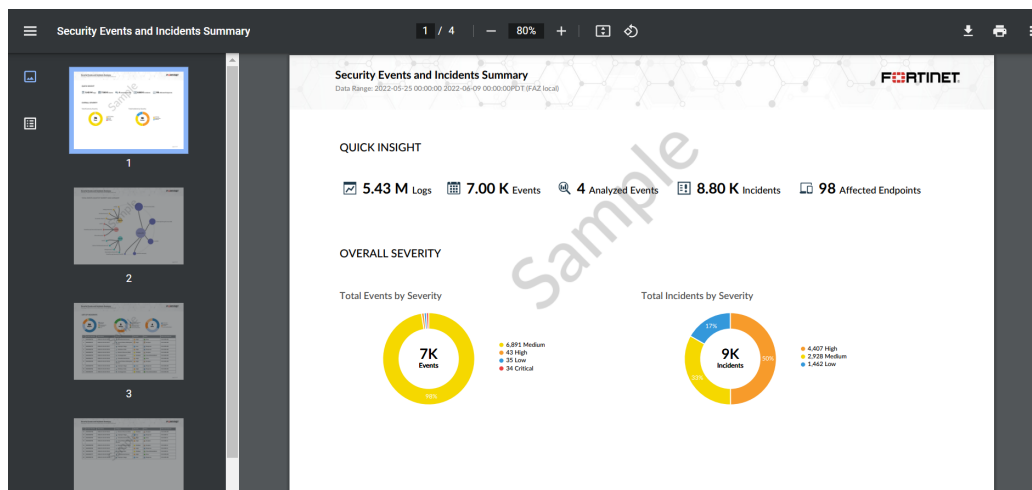


3. In the *Generated Reports* tab, click *Run Report*.
4. Once the report is generated, click a format in the *Format* column to view the report.

## Security events and incidents summary report update - 7.2.1

The *Security Events and Incidents Summary* report is updated to improve data visualization.

For example, below is a sample of the report in PDF format.

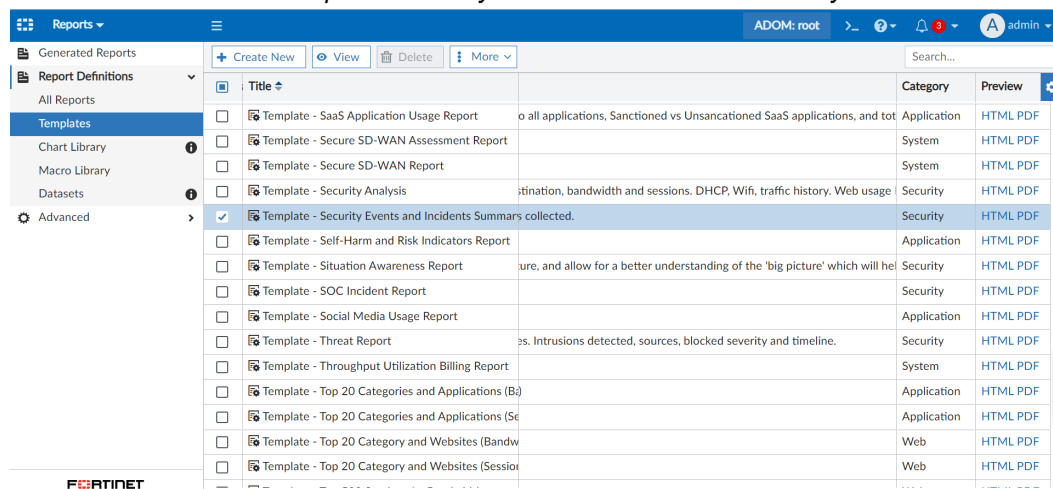


To use the Security Events and Incidents Summary report template:

1. Go to *Reports > Report Definitions > Templates*.

From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.

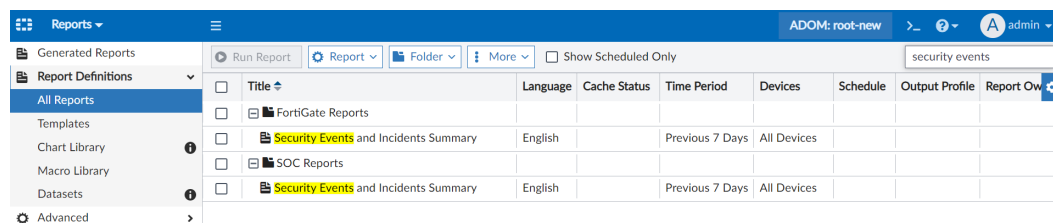
## 2. Select the checkbox for *Template - Security Events and Incidents Summary*.



- From the *More* dropdown, click *Clone* to clone the template and make adjustments. You can also click *Create Report* to create a report using the template.

## To run the Security Events and Incidents Summary report:

- Go to *Reports > Report Definitions > All Reports*.
- Double-click the row for *Security Events and Incidents Summary*. You can find the report using the search bar. For example, see the image below.

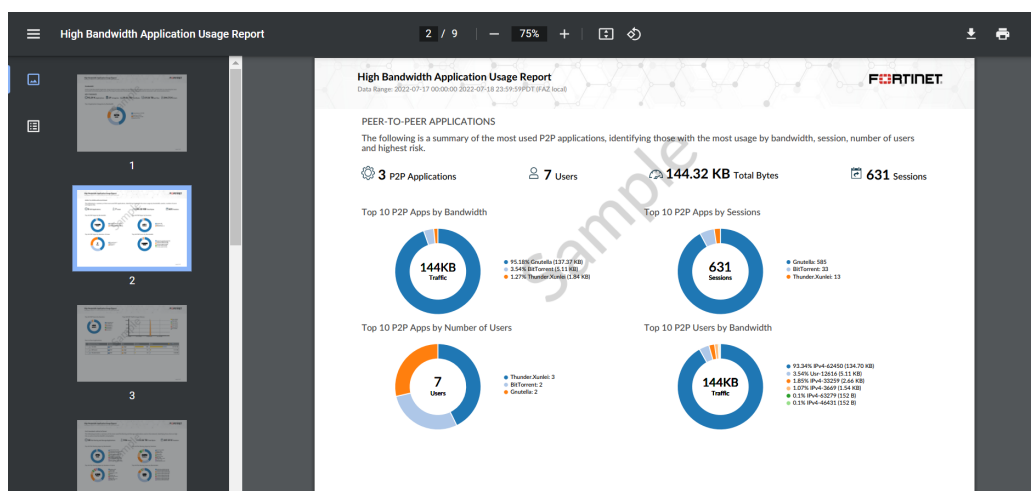
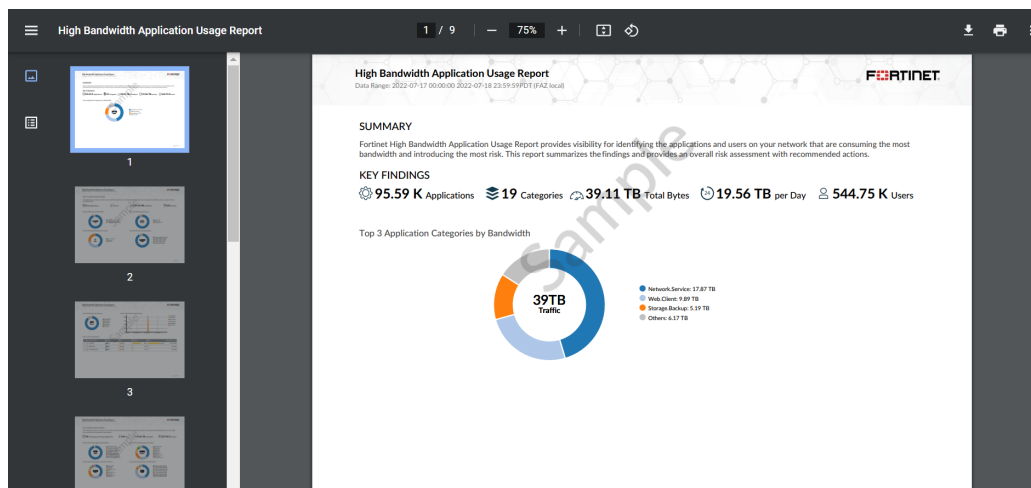


- In the *Generated Reports* tab, click *Run Report*.
- Once the report is generated, click a format in the *Format* column to view the report.

## High bandwidth application usage report update - 7.2.1

The *High Bandwidth Application Usage Report* is updated to improve data visualization.

For example, below is a sample of the report in PDF format.

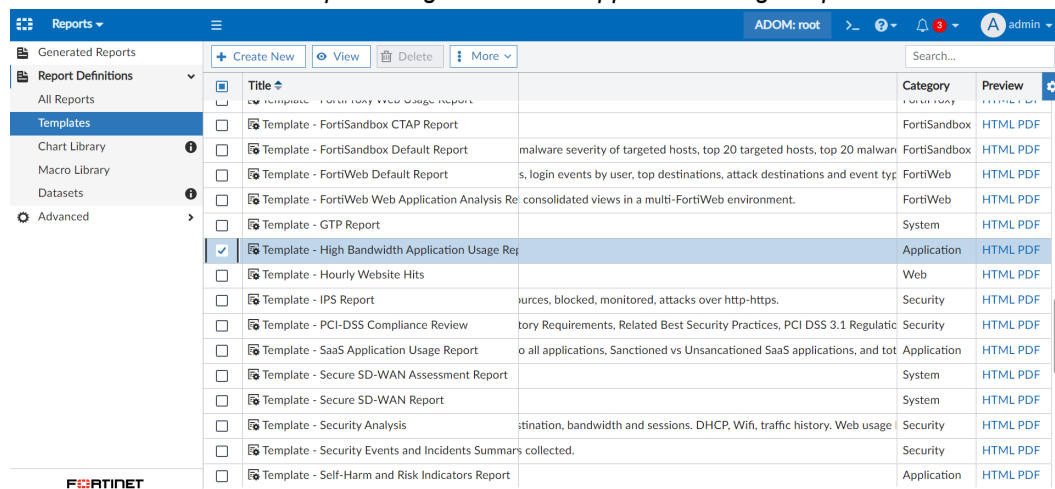


### To use the High Bandwidth Application Usage Report template:

1. Go to **Reports > Report Definitions > Templates**.  
From the *Preview* column, you can click **PDF** or **HTML** to preview the report in that format.



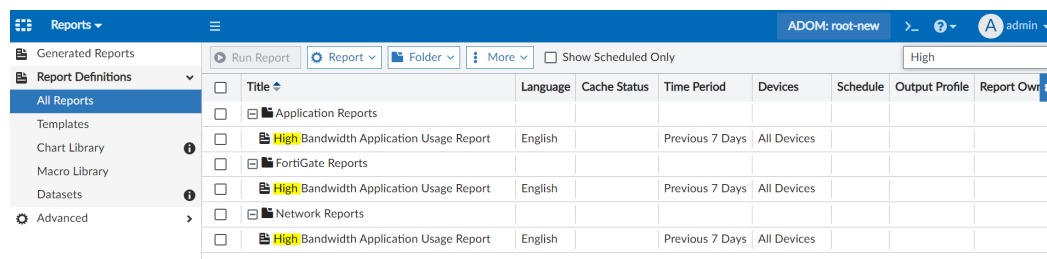
## 2. Select the checkbox for *Template - High Bandwidth Application Usage Report*.



- From the *More* dropdown, click *Clone* to clone the template and make adjustments. You can also click *Create Report* to create a report using the template.

## To run the High Bandwidth Application Usage Report:

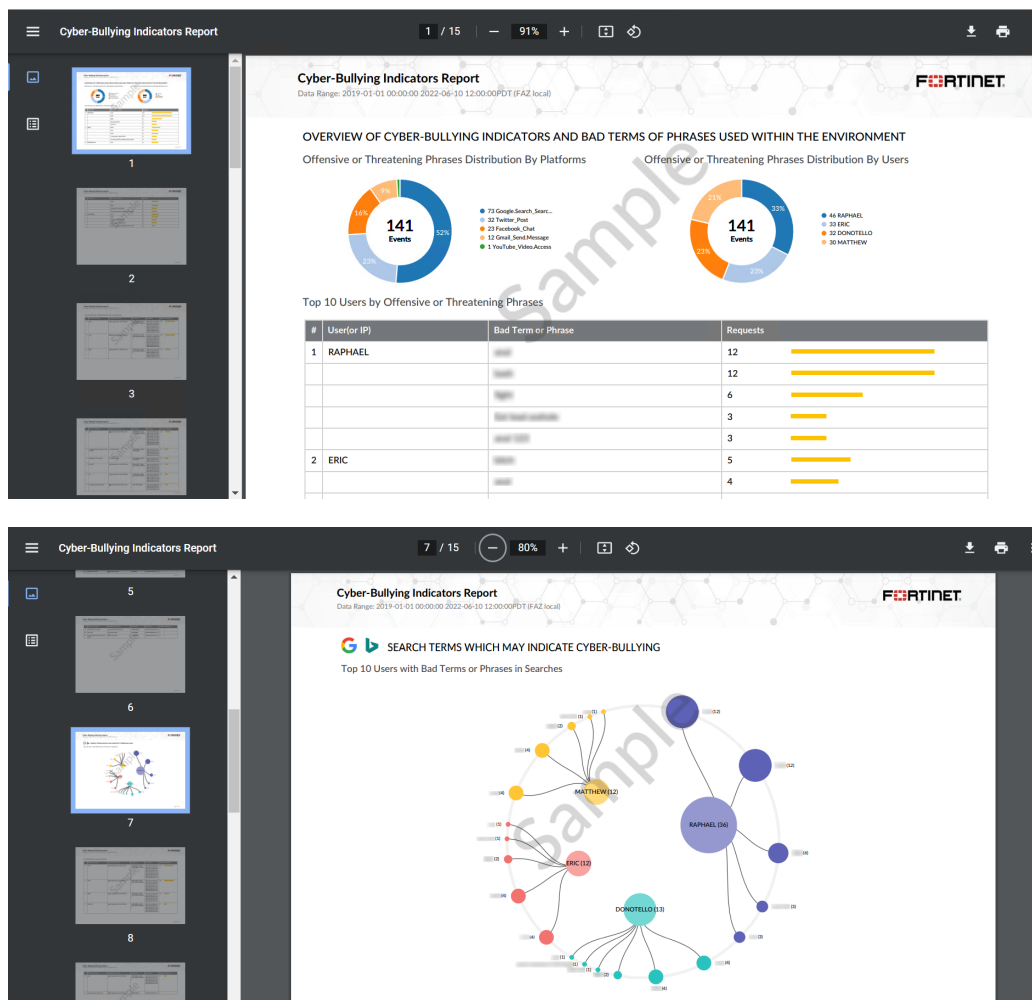
- Go to *Reports > Report Definitions > All Reports*.
- Double-click the row for *High Bandwidth Application Usage Report*. You can find the report using the search bar. For example, see the image below.



- In the *Generated Reports* tab, click *Run Report*.
- Once the report is generated, click a format in the *Format* column to view the report.

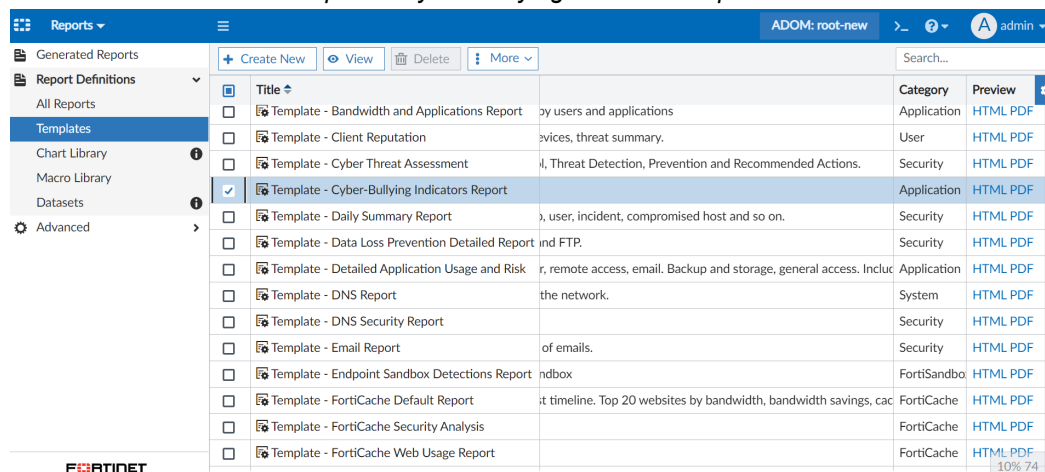
## Cyber-bullying indicators report update - 7.2.1

The content and style of the *Cyber-Bullying Indicators Report* is updated to improve data visualization. For example, below is a sample of the report in PDF format.



### To use the Cyber-Bullying Indicators Report template:

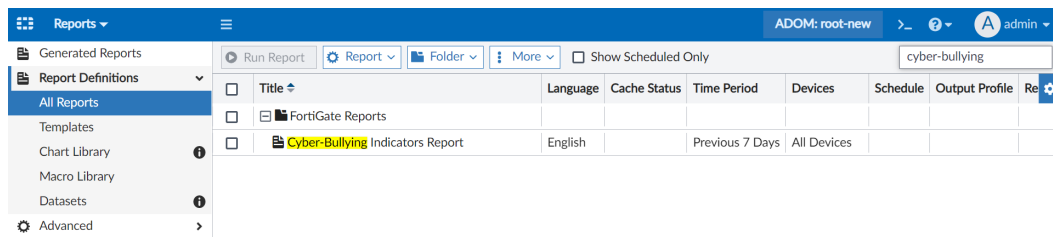
1. Go to *Reports > Report Definitions > Templates*.  
From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Cyber-Bullying Indicators Report*.



- From the *More* dropdown, click *Clone* to clone the template and make adjustments. You can also click *Create Report* to create a report using the template.

### To run the Cyber-Bullying Indicators Report:

- Go to *Reports > Report Definitions > All Reports*.
- Double-click the row for *Cyber-Bullying Indicators Report*. You can find the report using the search bar. For example, see the image below.

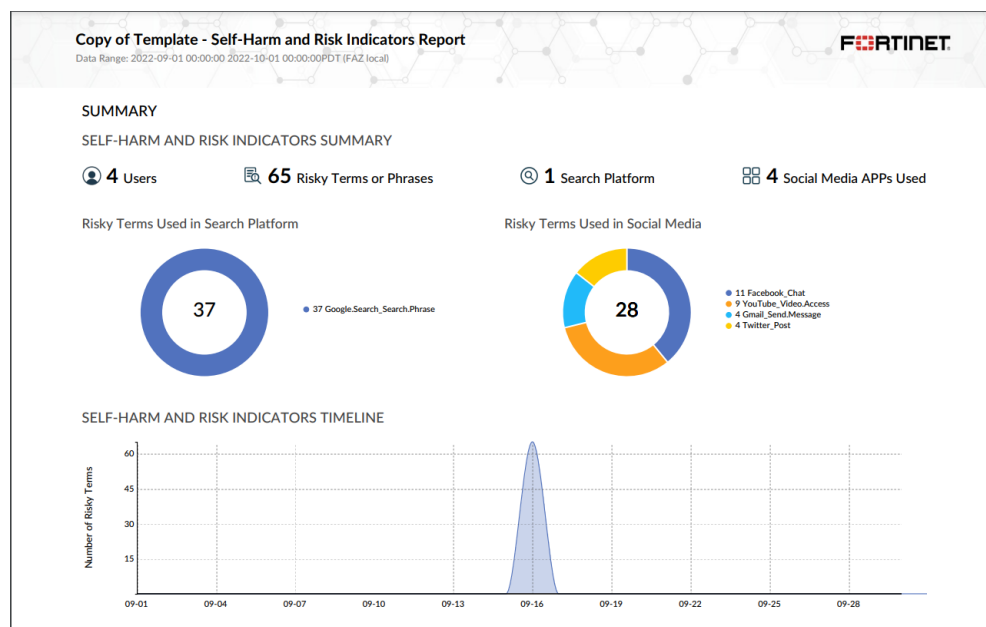


- In the *Generated Reports* tab, click *Run Report*.
- Once the report is generated, click a format in the *Format* column to view the report.

## Self-harm and risk indicators report update - 7.2.2

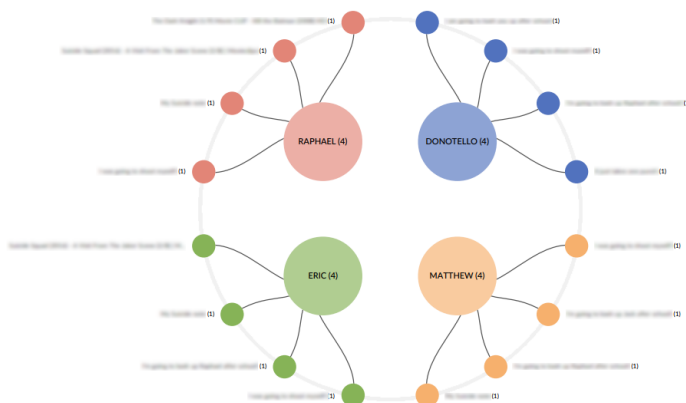
The *Self-Harm and Risk Indicators Report* is updated to improve data visualization.

For example, below is a sample of the report in PDF format.





TOP 10 USERS WITH RISKY TERMS OR PHRASES



### To use the Self-Harm and Risk Indicators Report template:

1. Go to *Reports > Report Definitions > Templates*.  
From the *Preview* column, you can click *PDF* or *HTML* to preview the report in that format.
2. Select the checkbox for *Template - Self-Harm and Risk Indicators Report*.
3. Right-click the template to select *Create Report*.  
You can also select *Clone* to clone the template and make adjustments.

Reports

Generated Reports

Report Definitions

All Reports

Templates

Chart Library

Macro Library

Datasets

Advanced

Create New

View

Delete

More

Search...

	Title	Language	Description	Category	Preview
<input type="checkbox"/>	Template - SaaS Application Usage Report	en	Summarizes the usage of SaaS apps compared to all applications	Application	HTML PDF
<input type="checkbox"/>	Template - Secure SD-WAN Assessment Report	en	Secure SD-WAN Assessment Report.	System	HTML PDF
<input type="checkbox"/>	Template - Secure SD-WAN Report	en	Secure SD-WAN Report.	System	HTML PDF
<input type="checkbox"/>	Template - Security Analysis	en	Security Analysis of traffic, application, user, destination, bandwidth	Security	HTML PDF
<input type="checkbox"/>	Template - Security Events and Incidents Summary	en	Present a brief summary of the events/incidents collected.	Security	HTML PDF
<input checked="" type="checkbox"/>	Template - Self-Harm and Risk Indicators Report	en	Self-Harm and Risk Indicators Report.	Application	HTML PDF
<input type="checkbox"/>	Template - Situation Awareness	en	Provide awareness of your current security posture, and allow for	Security	HTML PDF
<input type="checkbox"/>	Template - SOC Incident Report	en	Present a brief summary of SOC incidents.	Security	HTML PDF
<input type="checkbox"/>	Template - Social Media Usage	en	Social Media Usage Report.	Application	HTML PDF
<input type="checkbox"/>	Template - Threat Report	en	Malware, Botnets - detected, victims and sources. Intrusions detected	Security	HTML PDF
<input type="checkbox"/>	Template - Throughput Utilization Billing Report	en	Interface Throughput Utilization Billing Report.	System	HTML PDF
<input type="checkbox"/>	Template - Top 20 Categories and Applications (Bandwidth)	en	Top 20 Categories and Applications (Bandwidth)	Application	HTML PDF
<input type="checkbox"/>	Template - Top 20 Categories and Applications (Session)	en	Top 20 Categories and Applications (Session)	Application	HTML PDF
<input type="checkbox"/>	Template - Top 20 Category and Websites (Bandwidth)	en	Top 20 Category and Websites (Bandwidth)	Web	HTML PDF
<input type="checkbox"/>	Template - Top 20 Category and Websites (Session)	en	Top 20 Category and Websites (Session)	Web	HTML PDF

View

Delete

Clone

Create Report

### To run the Self-Harm and Risk Indicators Report:

1. Go to *Reports > Report Definitions > All Reports*.
2. Double-click the row for *Self-Harm and Risk Indicators Report*.  
Alternatively, you can use the copy that you created from the template. You can find the report using the search bar.
3. In the *Generated Reports* tab, click *Run Report*.
4. Once the report is generated, click a format in the *Format* column to view the report.

## Others

This section lists the new features added to FortiAnalyzer for other topics relating to logging and reporting:

- [Use device metadata in datasets and reports on page 93](#)
- [Search by object names on page 95](#)
- [Generate system event log when daemon crashes 7.2.2 on page 96](#)

## Use device metadata in datasets and reports

Device metadata such as branch ID, device geo-location, device names, and organization names can now be used by datasets and reports to provide enriched information.

Below are steps to create and run a custom report with device metadata.

### To create a dataset that queries the device metadata:

1. Go to *Reports > Report Definitions > Datasets*, and click *Create New*.
2. Configure a custom dataset to query logs and device metadata.
3. Click *Go* to test the output of the query.
4. If there are no errors to fix in the *Query*, click *OK* to save the dataset.

**Create Dataset**

Name: device metadata

Log Type: Event

Query:

```
1 select t1.devname, t2.platform, t2.organization,
t2.address, t2.phone, t2.email from ###(select devname
from $log group by devname)### t1 inner join
$ADOMTBL_PLHD_DEVMETA t2 on t1.devname=t2.name group by
t1.devname, t2.platform, t2.organization, t2.address,
t2.phone, t2.email order by t1.devname
```

Buttons: Validate, Analyze Query, Format

Variables:

Variable	Expression	Description
Click here to add new entry.		

Buttons: Go, Stop

Time Period: Previous 7 Days

Devices: All Devices

devname	platform	organization	address	phone	email
FGT101F-HA	FortiGate-101F	Fortinet	Still Creek		

Buttons: OK, Cancel

### To create a chart using the dataset with device metadata:

1. Go to *Reports > Report Definitions > Chart Library*, and click *Create New*.
2. In the *Name* field, type a name for the chart.
3. From the *Dataset* dropdown, select the dataset created with device metadata.
4. Configure the chart, and click *OK*.

See the [FortiAnalyzer Administration Guide](#) for more information about creating charts. Use the preview chart to review the chart as it is configured.

**Create Chart**

**Common**

Name: Device Metadata

Description:

Dataset: device metadata

Resolve Hostname: Inherit

Type: Table

Table Type: ☒ Regular ☐ Ranked ☐ Drilldown

Order By:

Show Top (0 for all): 10

**Regular Columns**

Column 1

Title: devname

Width: 0

% (0 for Auto)

Data Binding: devname

Format: Default

Preview table:

#	devname	platform	organization	address	phone	email
1	FG100	FortiGate	Fortinet	Still Creek	██████	██████
2	FGT-5	FortiGate	Fortinet	Still Creek	██████	██████
3	FGT-C	FortiGate	Fortinet	Still Creek	██████	██████
4	FGT10	FortiGate	Fortinet	Still Creek	██████	██████
5	FGT40	FortiGate	Fortinet	Still Creek	██████	██████
6	FWF-6	FortiWiFi	Fortinet	Robson St	██████	██████

Preview chart is for illustration purpose only. Actual report chart may vary from preview chart.

OK Cancel

### To create and run a report using the device metadata chart:

1. Go to *Reports > Report Definitions > All Reports*.
2. From the *Report* dropdown in the toolbar, click *Create New*.  
You can also edit an existing or cloned report to use this chart according to your needs.
3. Configure a name and folder location for the report.  
In this example, the report name is *Device Metadata Report*.
4. Go to the *Editor* tab for the report, and click *Insert Chart*.  
The *Insert Chart* dialog opens.
5. From the *Chart* dropdown, select the chart that uses the device metadata.
6. Click *OK*.

**Edit: Device Metadata Report**

Generated Reports Settings Editor

Insert Chart

Chart: All Device Metadata

Title: (default)

Width(1px - 900px):

Filters:

Log Field Match Criteria Value

Click here to add a new filter.

OK Cancel

Apply Return

7. Configure other settings for the report, and click *Apply* to save the report.  
See the [FortiAnalyzer Administration Guide](#) for more information about creating custom reports.
8. Go to the *Generated Reports* tab, and click *Run Report*.
9. Once the report is generated, click the *Format* you would like to download the report in.  
Below is an example of a PDF report with device metadata.

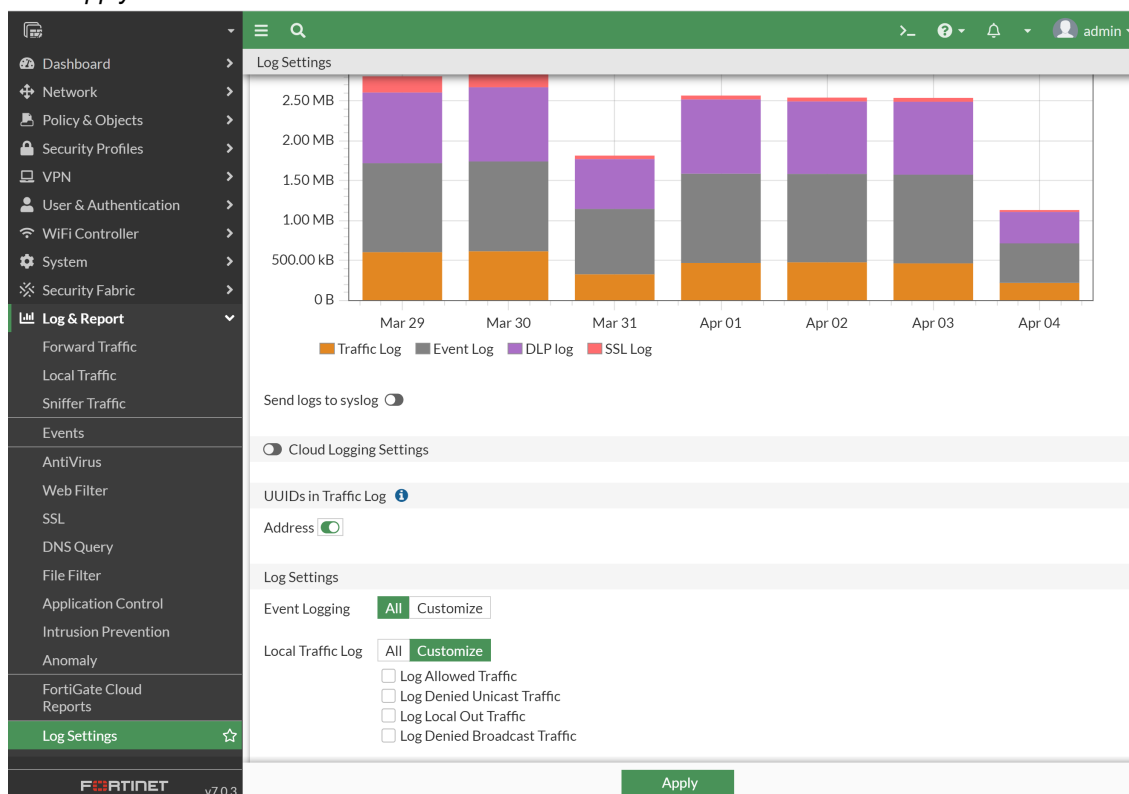
Device Metadata					
#	Device Name	Platform	Organization	Address	Phone Email
1	FGT100D3G1480B004	FortiGate-100D	Fortinet	Still Creek Drive 4190, Burnaby, British Columbia, Canada	5555555555555555
2	FGT-51E	FortiGate-51E	Fortinet	Still Creek Drive 310-4260, Burnaby, British Columbia, Canada	5555555555555555
3	FGT-CSF-Root	FortiGate-140D-POE	Fortinet	Still Creek Drive 4190, Burnaby, British Columbia, Canada	5555555555555555
4	FGT101F-HA	FortiGate-101F	Fortinet	Still Creek Drive 310-4260, Burnaby, British Columbia, Canada	5555555555555555
5	FGT40F	FortiGate-40F	Fortinet	Still Creek Drive 4190, Burnaby, British Columbia, Canada	5555555555555555
6	PWF-61F	FortiWiFi-61F	Fortinet	Robson Street 800, Vancouver, British Columbia, Canada	5555555555555555

## Search by object names

Source Object and Destination Object filters are now available to simplify search. The FortiAnalyzer admin can select an object filter and specify an object name to search *Log View* and *FortiView*.

To enable this feature from the FortiGate device:

1. In the FortiOS GUI, go to *Log & Report > Log Settings*.
2. Under *UUIDs in Traffic Log*, enable *Address*.
3. Click *Apply*.



## Examples using the filters in FortiAnalyzer:

- *Log View > FortiGate > Traffic* filtered by Source Object and Destination Object. These filters are available for traffic logs and utm logs. The *Destination Object* and *Source Object* columns are added.

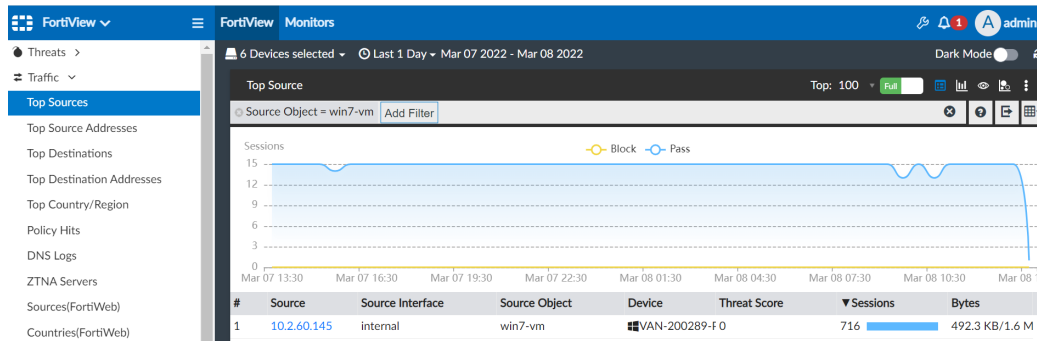
Log View

6 Devices selected | Last 1 Day | Mar 07 To Mar 08

Source Object = "net-remote" | Destination Object = "net-localY" | Add Filter

#	Date/Time	Device ID	Action	Source	Destination IP	Service	Application	Sent/Received	Destination Object	Source Object
1	13:24:45	FGT91E4...	✓	192.16...	10.2.60.104	tcp/514	tcp/514	16.1 M...	net-localY	net-remote
2	13:23:10	FGT91E4...	✓	192.16...	10.2.60.104	SYSLOG	SYSLOG	7.1 MB...	net-localY	net-remote
3	13:22:40	FGT91E4...	✓	192.16...	10.2.60.104	tcp/514	tcp/514	16.1 M...	net-localY	net-remote
4	13:21:10	FGT91E4...	✓	192.16...	10.2.60.104	SYSLOG	SYSLOG	7.1 MB...	net-localY	net-remote
5	13:20:40	FGT91E4...	✓	192.16...	10.2.60.104	tcp/514	tcp/514	16.1 M...	net-localY	net-remote

- **FortiView > Traffic > Top Sources** filtered by Source Object. The Source Object column is added.



- **FortiView > Traffic > Top Source Addresses** filtered by Source Object.

FortiView Monitors

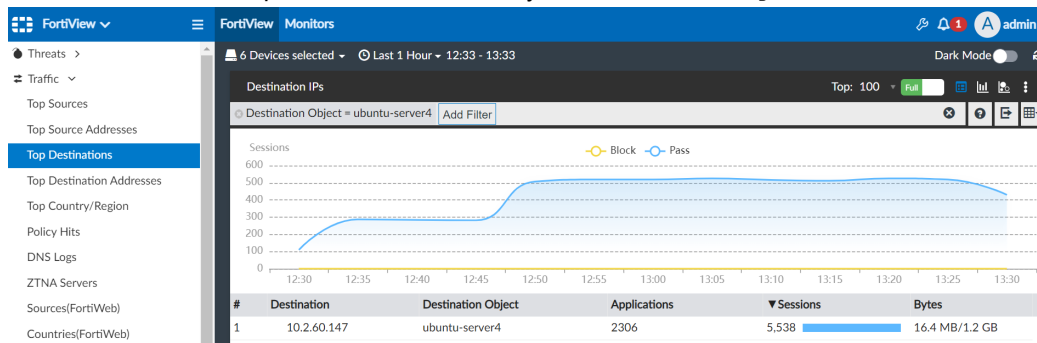
All Devices | Last 1 Hour | 12:28 - 13:28

Top Source Address Objects

Source Object = SSLVPN\_TUNNEL\_ADDR1 | Add Filter

#	Source Object	Source Interface	Device	Threat Score	Sessions
1	SSLVPN_TUNNEL_ADDR1 ssl.root			0	2,584

- **FortiView > Traffic > Top Destinations** filtered by Destination Object.



- **FortiView > Traffic > Top Destination Addresses** filtered by Destination Object. The Destination Object column is added.

FortiView Monitors

All Devices | Last 1 Hour | 12:29 - 13:29

Top Destination Address Objects

Destination Object = Private\_IP\_Range\_Group | Add Filter

#	Destination Object	Applications	Sessions	Bytes
1	Private_IP_Range_Group	7	125	34.9 KB/34.9 KB

## Generate system event log when daemon crashes - 7.2.2

You can now enable, via CLI, the functionality to generate a system event log when a daemon crashes.



These event logs are generated with *level=warning* and the entire backtrace is included in the *msg* field.

To generate a system event log when a daemon crashes, you must enable `log-daemon-crash` in the FortiAnalyzer CLI.

### To generate a system event log when a daemon crashes:

1. Enter the following command in the FortiAnalyzer CLI:

```
config system locallog setting
  set log-daemon-crash enable
end
```



By default, `log-daemon-crash` is set to `disable`. When disabled, a system event log is not generated when a daemon crashes.

---

### To view the system event logs for daemon crashes:

1. In the FortiAnalyzer GUI, go to *System Settings > Event Log*.



You can also check crash logs by entering the following command in the FortiAnalyzer CLI:

```
diagnose debug crashlog read
```

---

# System

This section lists the new features added to FortiAnalyzer for system settings:

- [High Availability \(HA\) on page 98](#)
- [Administrators on page 101](#)
- [Network on page 103](#)
- [Others on page 105](#)

## High Availability (HA)

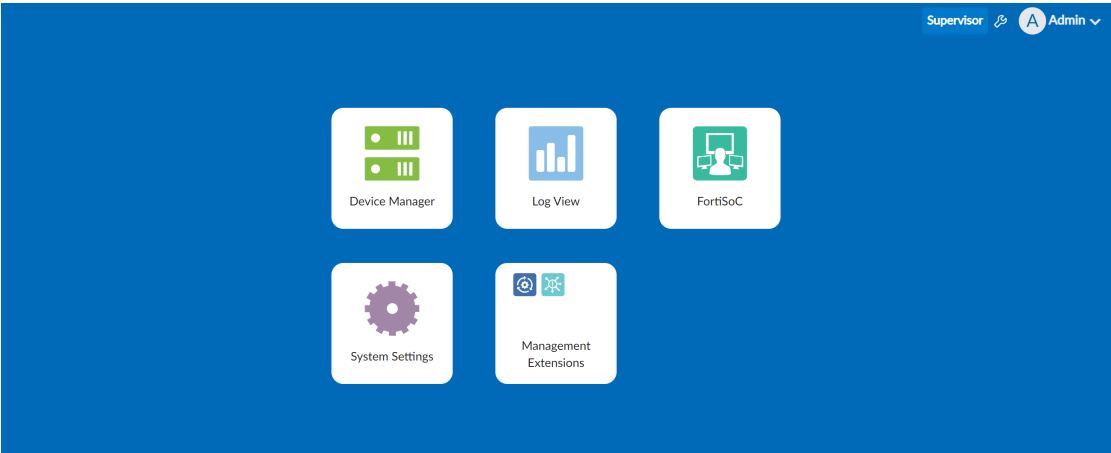
This section lists the new features added to FortiAnalyzer for high availability (HA):

- [Global log search across FortiAnalyzer Fabric members 7.2.1 on page 98](#)

## Global log search across FortiAnalyzer Fabric members - 7.2.1

The *Log View* pane is added to the FortiAnalyzer Fabric supervisor.

This *Log View* supports a global search of logs collected across FortiAnalyzer Fabric members. The supervisor displays the same information about the logs as displayed in the FortiAnalyzer Fabric member that they were collected on.



Two columns are added in the supervisor's *Log View* to identify where the logs were collected:

<b>FortiAnalyzer Host Name</b>	The host name for the FortiAnalyzer device that collected the log. To find or edit the <i>Host Name</i> for a FortiAnalyzer Fabric member, go to <i>System Settings &gt; Dashboard &gt; System Information</i> in the GUI for the member device.
<b>ADOM</b>	The ADOM that the log was generated in.

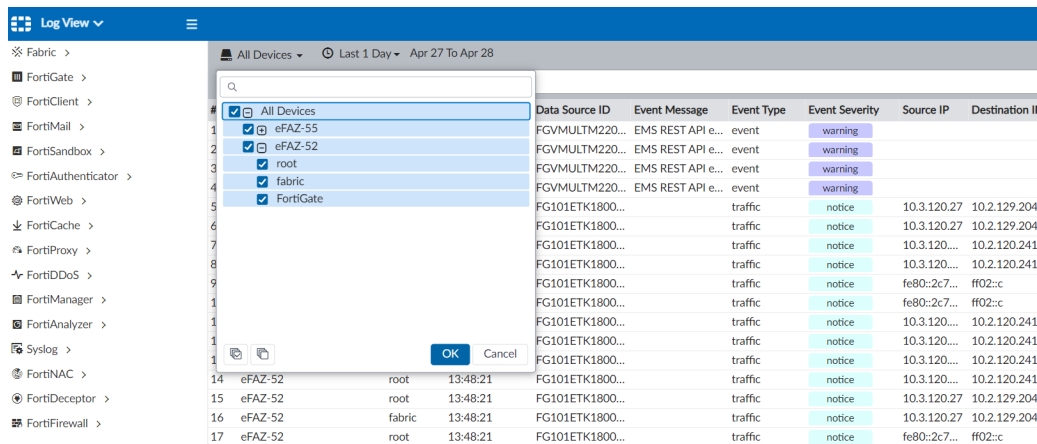
#	FortiAnalyzer Host Name	ADOM	Date/Time	Data Source ID	Event Message	Event Type	Event Severity	Source IP	Destination IP	Host Name	User ID	App
1	eFAZ-52	fabric	13:48:26	FGVMULTM220...	EMS REST API e...	event	warning					
2	eFAZ-52	root	13:48:26	FGVMULTM220...	EMS REST API e...	event	warning					
3	eFAZ-52	fabric	13:48:26	FGVMULTM220...	EMS REST API e...	event	warning					
4	eFAZ-52	root	13:48:26	FGVMULTM220...	EMS REST API e...	event	warning					
5	eFAZ-52	fabric	13:48:21	FG101ETK1800...		traffic	notice	10.3.120.27	10.2.129.204	10.3.120.27		
6	eFAZ-52	root	13:48:21	FG101ETK1800...		traffic	notice	10.3.120.27	10.2.129.204	10.3.120.27		
7	eFAZ-52	root	13:48:21	FG101ETK1800...		traffic	notice	10.3.120...	10.2.120.241	DESKTOP-8...		
8	eFAZ-52	fabric	13:48:21	FG101ETK1800...		traffic	notice	10.3.120...	10.2.120.241	DESKTOP-8...		
9	eFAZ-52	fabric	13:48:21	FG101ETK1800...		traffic	notice	fe80::2c7...	ff02::c		Win7QA	udp/...
10	eFAZ-52	root	13:48:21	FG101ETK1800...		traffic	notice	fe80::2c7...	ff02::c		Win7QA	udp/...
11	eFAZ-52	fabric	13:48:21	FG101ETK1800...		traffic	notice	10.3.120...	10.2.120.241	DESKTOP-8...		
12	eFAZ-52	root	13:48:21	FG101ETK1800...		traffic	notice	10.3.120...	10.2.120.241	DESKTOP-8...		
13	eFAZ-52	fabric	13:48:21	FG101ETK1800...		traffic	notice	10.3.120...	10.2.120.241	DESKTOP-8...		
14	eFAZ-52	root	13:48:21	FG101ETK1800...		traffic	notice	10.3.120...	10.2.120.241	DESKTOP-8...		
15	eFAZ-52	root	13:48:21	FG101ETK1800...		traffic	notice	10.3.120.27	10.2.129.204	10.3.120.27		
16	eFAZ-52	fabric	13:48:21	FG101ETK1800...		traffic	notice	10.3.120.27	10.2.129.204	10.3.120.27		
17	eFAZ-52	root	13:48:21	FG101ETK1800...		traffic	notice	fe80::2c7...	ff02::c		Win7QA	udp/...
18	eFAZ-52	fabric	13:48:21	FG101ETK1800...		traffic	notice	fe80::2c7...	ff02::c		Win7QA	udp/...
19	eFAZ-52	root	13:48:21	FG101ETK1800...		traffic	notice	10.3.120.27	10.2.129.204	10.3.120.27		
20	eFAZ-52	fabric	13:48:21	FG101ETK1800...		traffic	notice	10.3.120.27	10.2.129.204	10.3.120.27		
21	eFAZ-52	root	13:48:21	FG101ETK1800...		traffic	notice	10.3.120.27	10.2.129.204	10.3.120.27		
22	eFAZ-52	fabric	13:48:21	FG101ETK1800...		traffic	notice	10.3.120.27	10.2.129.204	10.3.120.27		

The **Log View** in a FortiAnalyzer Fabric supervisor does not support *Log Group*, *Log Browse*, *Log Downloads*, *Custom View*, or *Chart Builder*. These features are available in FortiAnalyzer Fabric members and regular FortiAnalyzer devices. For more information, see the FortiAnalyzer Administration Guide.

#	FortiAnalyzer Host Name	ADOM	Date/Time	Device ID	Action	Source	User	Destination IP	Service
1	eFAZ-52	fabric	10:03:42	FGVULVTM2...	✓	10.3.120.201		10.2.120.241	tcp/8000
2	eFAZ-52	fabric	10:03:41	FGVULVTM2...	✓	DESKTOP...		52.226.139.185	HTTPS
3	eFAZ-52	fabric	10:03:41	FGVULVTM2...	Policy vi...	fe80::2c76...		ff02::c	udp/1900
4	eFAZ-52	fabric	10:03:41	FGVULVTM2...	Policy vi...	fe80::2c76...		ff02::c	udp/1900
5	eFAZ-52	fabric	10:03:41	FGVULVTM2...	Policy vi...	fe80::2c76...		ff02::c	udp/1900
6	eFAZ-52	fabric	10:03:41	FGVULVTM2...	Policy vi...	fe80::2c76...		ff02::c	udp/1900
7	eFAZ-52	fabric	10:03:41	FGVULVTM2...	Policy vi...	fe80::2c76...		ff02::c	udp/1900
8	eFAZ-52	fabric	10:03:40	FGVULVTM2...	✓	10.3.120.201		10.2.120.241	tcp/8000
9	eFAZ-52	fabric	10:03:39	FGVULVTM2...	✓	DESKTOP...		142.251.33.78	HTTPS
10	eFAZ-52	fabric	10:03:38	FGVULVTM2...	✓	10.3.120.201		10.2.120.241	tcp/8000
11	eFAZ-52	fabric	10:03:38	FGVULVTM2...	Policy vi...	fe80::2c76...		ff02::c	udp/1900
12	eFAZ-52	fabric	10:03:38	FGVULVTM2...	Policy vi...	fe80::2c76...		ff02::c	udp/1900
13	eFAZ-52	fabric	10:03:38	FGVULVTM2...	Policy vi...	fe80::2c76...		ff02::c	udp/1900
14	eFAZ-52	fabric	10:03:38	FGVULVTM2...	Policy vi...	fe80::2c76...		ff02::c	udp/1900
15	eFAZ-52	fabric	10:03:38	FGVULVTM2...	Policy vi...	fe80::2c76...		ff02::c	udp/1900

### To use **Log View** in a FortiAnalyzer Fabric supervisor:

1. Confirm you are in the FortiAnalyzer Fabric supervisor.
2. Go to **Log View**.
3. From the **Device Filter** dropdown, select the FortiAnalyzer Fabric members and ADOMs to display logs from, and click **OK**.



4. In the search bar, type the filters to apply to the table, and click the search icon.

The search bar supports a global search across all FortiAnalyzer Fabric members. The *FortiAnalyzer Host Name* and *ADOM* columns display where the log was originally collected in the FortiAnalyzer Fabric.

#	FortiAnalyzer Host Name	ADOM	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Security Event List
1	eFAZ-52	root	13:55:02	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
2	eFAZ-52	root	13:55:01	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
3	eFAZ-55	fabric	13:54:36	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
4	eFAZ-52	root	13:54:36	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
5	eFAZ-52	root	13:54:32	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
6	eFAZ-55	fabric	13:54:32	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
7	eFAZ-55	fabric	13:54:32	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
8	eFAZ-52	root	13:54:32	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
9	eFAZ-55	fabric	13:54:31	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
10	eFAZ-52	root	13:54:31	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
11	eFAZ-55	fabric	13:54:17	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
12	eFAZ-52	root	13:54:17	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
13	eFAZ-52	root	13:54:16	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
14	eFAZ-55	fabric	13:54:16	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
15	eFAZ-55	fabric	13:54:16	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	
16	eFAZ-52	root	13:54:16	FGVMULTM22000748	✓	10.3.120.207		10.3.120.240	HTTPS	HTTPS	

## To download FortiGate archive files for security logs from a FortiAnalyzer Fabric supervisor:

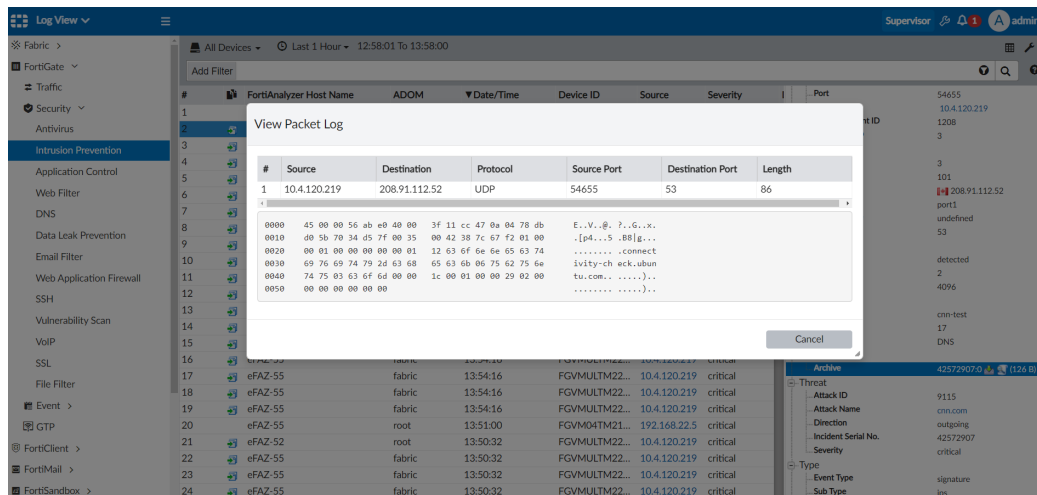
1. Confirm you are in the FortiAnalyzer Fabric supervisor.
2. Go to *Log View > FortiGate > Security > Intrusion Prevention*.

In this example, the administrator downloads archive files for intrusion prevention. The same steps can be used from other log types available under *Log View > FortiGate > Security*.

3. Double-click the archive log to download.

The log details pane displays.

4. In the *Archive* field, click the download icon.



## Administrators

This section lists the new features added to FortiAnalyzer for administrators:

- [Add French language support to GUI on page 101](#)

## Add French language support to GUI

FortiAnalyzer GUI now supports French in addition to the previously supported languages.

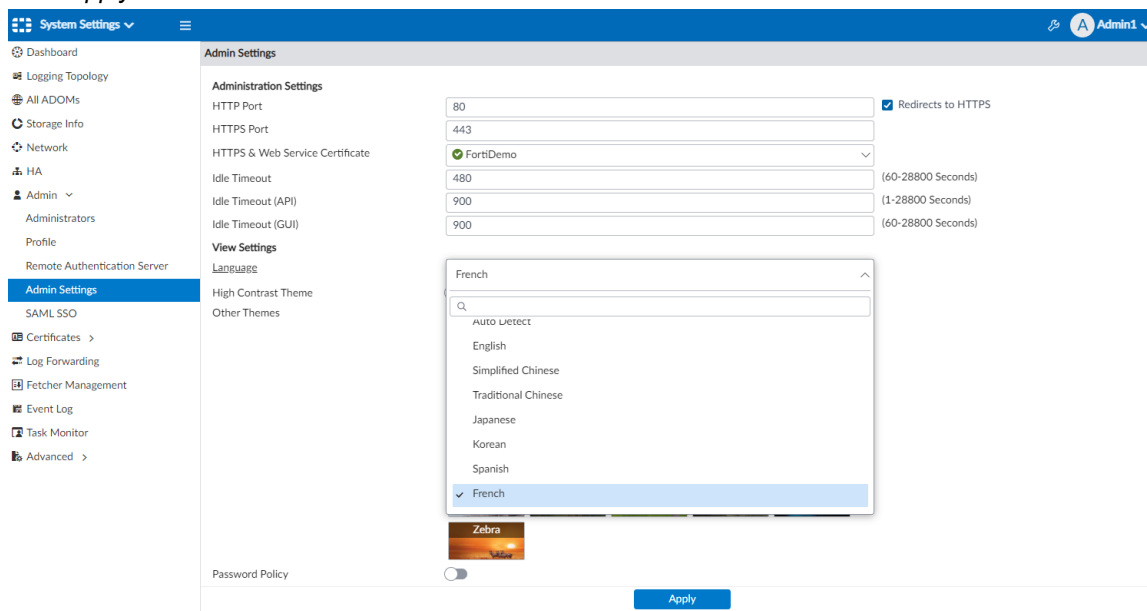


By default, the GUI language is set to *Auto Detect*, which automatically uses the language set for the administrator's browser. If that language is not supported, the GUI defaults to English.

### To set the GUI language to French:

1. Go to *System Settings > Admin > Admin Settings*.
2. From the *Language* dropdown, select *French*.

### 3. Click *Apply*.

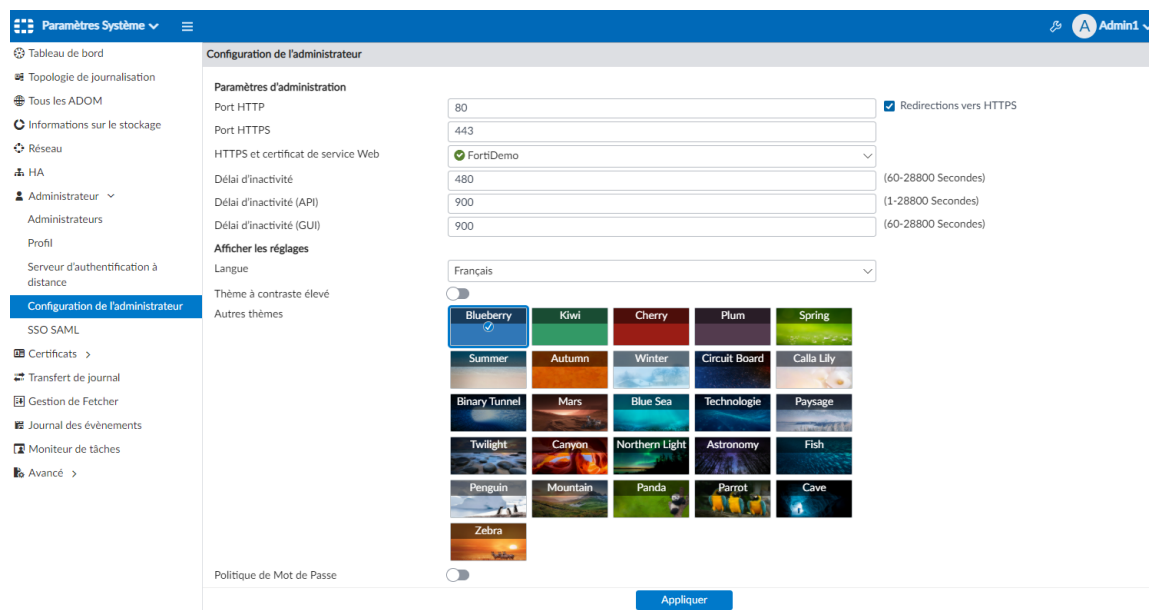


### To set the GUI language to French from the CLI:

```
config system admin setting
    set webadmin_language french
end
```

This setting does not affect the CLI.

Below is an example of the French GUI:



## Network

This section lists the new features added to FortiAnalyzer for networks:

- FortiAnalyzer supports VLANs on physical network interfaces on page 103

### FortiAnalyzer supports VLANs on physical network interfaces

FortiAnalyzer supports VLANs on physical network interfaces.

#### To create a VLAN on FortiAnalyzer:

- Go to *System Settings > Network*, and click *Create New* in the *Interface* table toolbar. The Create New Network Interface window opens.
- Select VLAN as the interface type, and enter the VLAN name, VLAN ID, and the interface to which the VLAN is bound.

The screenshot shows the 'Create New Network Interface' window in FortiAnalyzer. On the left, the 'Network' sidebar is visible, showing the 'Interface' table with a 'Create New' button. The main window has the following fields:

- Name:** VLAN10
- Alias:** (empty)
- Type:** VLAN (selected from a dropdown)
- VLAN ID:** 10 (selected from a dropdown, with a range of 1-4094 shown)
- Interface:** port2 (selected from a dropdown)
- Protocol:** IEEE 802.1Q (selected from a dropdown)
- IP Address/Netmask:** 10.10.1.1/255.255.0.0
- IPv6 Address:** ::/0
- Administrative Access:**
  - ☒ HTTPS ☒ HTTP ☒ PING ☐ SSH ☐ SNMP ☐ Web Service ☐ FortiManager
  - ☐ HTTPS ☐ HTTP ☐ PING ☐ SSH ☐ SNMP ☐ Web Service ☐ FortiManager
- IPv6 Administrative Access:** (empty)
- Service Access:**
  - ☐ FortiGate Updates
  - ☐ Web Filtering
- Status:** Enable (selected from a dropdown)
- Description:** (empty text area)

At the bottom of the window are 'OK' and 'Cancel' buttons.

- Click **OK** to save the VLAN. The VLAN is visible on the network page.

**Network**

**Interface**

+ Create New Edit Delete Column Settings Search...

<input type="checkbox"/>	Name	Type	Members/Interface	IP/Netmask	IPv6 Address
<input type="checkbox"/>	port1	Physical Interface		10.100.55.12/255.255.255.0	::/0
<input type="checkbox"/>	port2	Physical Interface		10.100.88.12/255.255.255.0	::/0
<input type="checkbox"/>	port3	Physical Interface		0.0.0.0/0.0.0.0	::/0
<input type="checkbox"/>	port4	Physical Interface		0.0.0.0/0.0.0.0	::/0
<input type="checkbox"/>	port5	Physical Interface		0.0.0.0/0.0.0.0	::/0
<input type="checkbox"/>	port6	Physical Interface		0.0.0.0/0.0.0.0	::/0
<input type="checkbox"/>	port7	Physical Interface		0.0.0.0/0.0.0.0	::/0
<input type="checkbox"/>	port8	Physical Interface		0.0.0.0/0.0.0.0	::/0
<input type="checkbox"/>	port9	Physical Interface		0.0.0.0/0.0.0.0	::/0
<input type="checkbox"/>	port10	Physical Interface		0.0.0.0/0.0.0.0	::/0
<input type="checkbox"/>	port11	Physical Interface		0.0.0.0/0.0.0.0	::/0
<input type="checkbox"/>	port12	Physical Interface		0.0.0.0/0.0.0.0	::/0
<input type="checkbox"/>	test	Aggregate	port3, port4	192.168.50.242/255.255.255.0	::/0
<input type="checkbox"/>	VLAN10	VLAN	port2	10.10.1.1/255.255.0.0	::/0

**DNS**

Primary DNS Server

Secondary DNS Server

**Apply**

If required, you can create a static route using the VLAN interface.

**Network**

**Interface**

+ Create New Edit Delete

<input type="checkbox"/>	Name
<input type="checkbox"/>	port1
<input type="checkbox"/>	port2
<input type="checkbox"/>	port3
<input type="checkbox"/>	port4
<input type="checkbox"/>	port5
<input type="checkbox"/>	port6
<input type="checkbox"/>	port7
<input type="checkbox"/>	port8
<input type="checkbox"/>	port9
<input type="checkbox"/>	port10
<input type="checkbox"/>	port11
<input type="checkbox"/>	port12
<input type="checkbox"/>	test
<input type="checkbox"/>	VLAN10

**DNS**

Primary DNS Server

Secondary DNS Server

**Routing Table**

+ Create New Edit Delete

<input type="checkbox"/>	ID
<input type="checkbox"/>	1

**Create New Network Route**

IP Type

Destination IP/Mask

Gateway

Interface

**OK Cancel**

### To configure VLAN interfaces in the CLI:

1. Open the FortiAnalyzer CLI.
2. Enter the following commands.

```

config system interface
edit <vlan-name>
set type vlan
set interface "portx"
set vlanid <1-4094>
set vlan-protocol <8021q/8021ad>

```



```
end
```

For example:

```
config system interface
  edit "vlan2"
    set ip 2.2.2.2 255.255.255.0
    set allowaccess ping https ssh
    set type vlan
    set interface "port2"
    set vlanid 2
    set vlan-protocol 8021q
  end
```

## Others

This section lists the new features added to FortiAnalyzer for other features relating to system settings:

- [FortiAnalyzer Fabric usability improvements on page 105](#)
- [Add LLDP support on FMG and FAZ 7.2.1 on page 109](#)
- [Mandatory FortiCare/FortiCloud registration 7.2.1 on page 109](#)

## FortiAnalyzer Fabric usability improvements

*System Settings > FortiAnalyzer Fabric* is a new GUI to easily setup a FortiAnalyzer Fabric Cluster.

The supervisor node provides a centralized view for the whole cluster. Card style summary dashboards are available in the supervisor's *Device Manager*, and filters can be applied to those summary dashboards.

This topic includes:

- [Configuring a FortiAnalyzer Fabric from the GUI on page 105](#)
- [Viewing member devices from the FortiAnalyzer Fabric supervisor on page 107](#)

For more information about FortiAnalyzer Fabric, see the [FortiAnalyzer Fabric Deployment Guide](#).

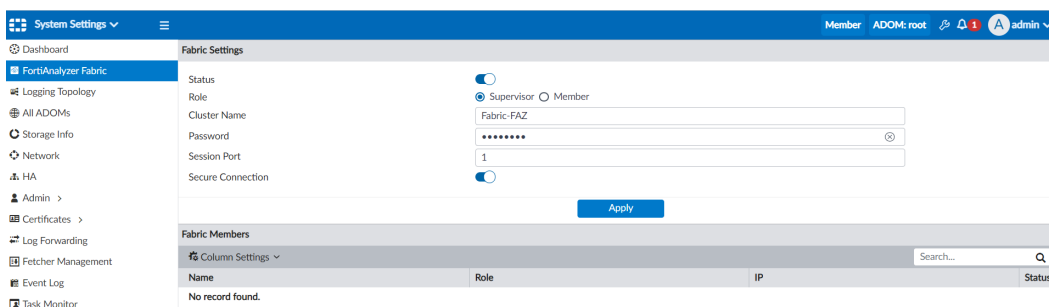
### Configuring a FortiAnalyzer Fabric from the GUI

**To configure a supervisor from the GUI:**

1. Confirm you are in the GUI for the FortiAnalyzer that will be the supervisor.
2. Go to *System Settings > FortiAnalyzer Fabric*.
3. Set *Status* to *enabled*.

4. Configure the following settings for the supervisor, and then click *Apply* to save.

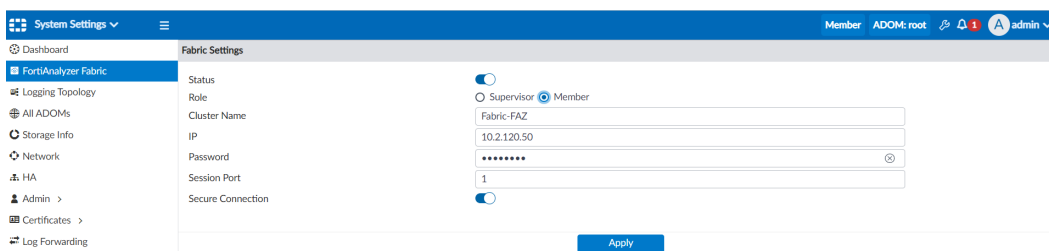
<b>Role</b>	Select <i>Supervisor</i> .
<b>Cluster Name</b>	Type a name for the FortiAnalyzer Fabric.
<b>Password</b>	Type a password for the FortiAnalyzer Fabric.
<b>Session Port</b>	Default = 6443. Type the communication port if not using the default.
<b>Secure Connection</b>	Enable or disable secure connection.



### To configure a member from the GUI:

1. Confirm you are in the GUI for the FortiAnalyzer that will be a member.
2. Go to *System Settings > FortiAnalyzer Fabric*.
3. Configure the following settings for the member, and then click *Apply* to save.

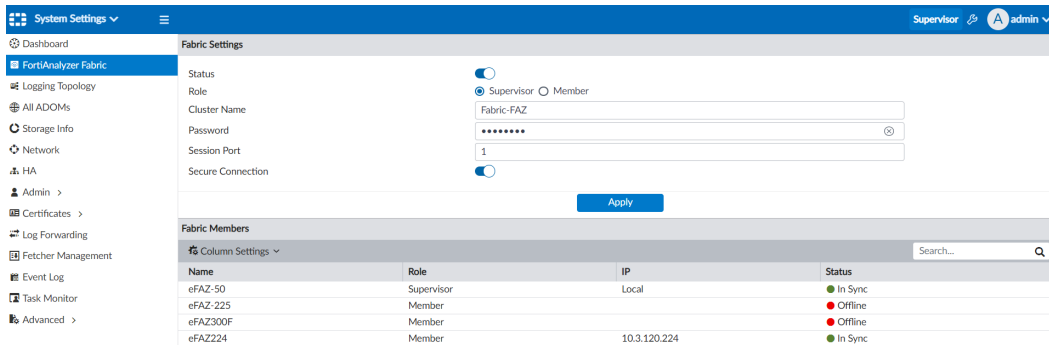
<b>Role</b>	Select <i>Member</i> .
<b>Cluster Name</b>	Type the name of the FortiAnalyzer Fabric.
<b>IP</b>	Type the IP of the supervisor for the FortiAnalyzer Fabric.
<b>Password</b>	Type the password configured for the FortiAnalyzer Fabric.
<b>Session Port</b>	Default = 6443. Type the communication port if not using the default.
<b>Secure Connection</b>	Enable or disable secure connection.



### To view the FortiAnalyzer Fabric from the supervisor:

1. Confirm you are in the GUI for the FortiAnalyzer Fabric supervisor.
2. Go to *System Settings > FortiAnalyzer Fabric*.  
Once the supervisor and members are connected and synchronized, the *Fabric Members* table includes the following information for each FortiAnalyzer in the FortiAnalyzer Fabric:

<b>Name</b>	The name of the FortiAnalyzer.
<b>Role</b>	The role of the FortiAnalyzer in the FortiAnalyzer Fabric (supervisor or member).
<b>IP</b>	The IP address of the FortiAnalyzer.
<b>Status</b>	The status of the FortiAnalyzer.



## Viewing member devices from the FortiAnalyzer Fabric supervisor

### To use the summary charts in Device Manager:

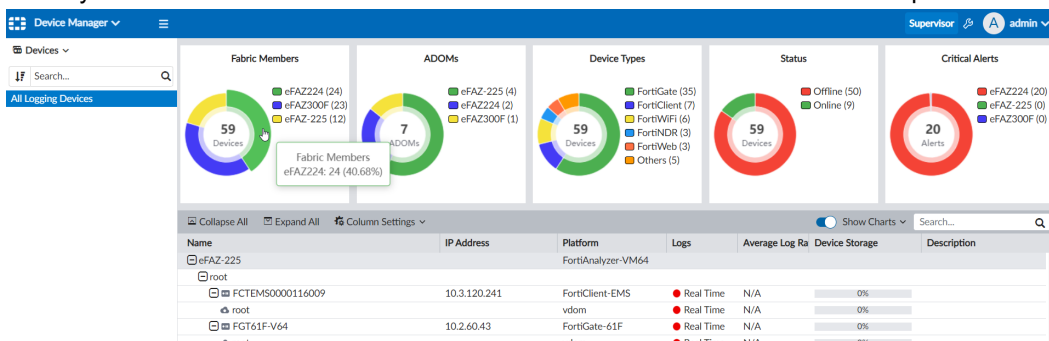
1. Confirm you are in the GUI for the FortiAnalyzer Fabric supervisor.
2. Go to *Device Manager*.

Five summary charts are available:

- *Fabric Members*
- *ADOMs*
- *Device Types*
- *Status*
- *Critical Alerts*

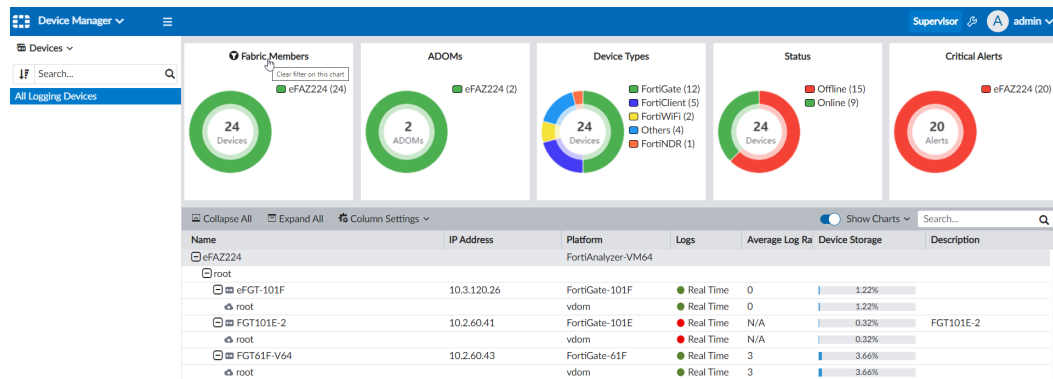
By default, the *Show Charts* toggle is enabled. You can select which charts appear by selecting them in the *Show Charts* dropdown, or you can hide all the charts by disabling the *Show Charts* toggle.

3. Hover your cursor over the charts to see more information about the data in a tooltip.



4. Click an area on a chart or in its legend to filter *Device Manager* by that information. You can click multiple charts and legends to apply multiple filters. A filter icon appears next to the chart title when it is being used to filter the *Device Manager*.

5. To remove the filters, click the title of the charts that were used.



### To use the table in Device Manager:

1. Confirm you are in the GUI for the FortiAnalyzer Fabric supervisor.
2. Go to *Device Manager*.

The table in the *Device Manager* provides the following information about each FortiAnalyzer Fabric member:

**Name** The name of the FortiAnalyzer Fabric member.

**Platform** The device's platform.

3. Click *Expand All*.

FortiAnalyzer Fabric member ADOMs are displayed below each member. Each ADOM includes their authorized logging devices. The following information is displayed for each device and VDOM in the table:

**Name** The name of the device.

**IP Address** The IP address of the device.

**Platform** The platform of the device.

**Logs** The real time log status.  
A green circle indicates that logs are being sent. A red circle indicates that logs are not being sent. The status indicator will turn from green to red when logs have not been sent for 15 minutes or longer.

**Average Log Rate (Logs/Sec)** The average log rate per second. This information is only available when the device is sending logs in real time.

**Device Storage** The amount of storage used by the device or VDOM.

Name	IP Address	Platform	Logs	Average Log Ra	Device Storage	Description
eFAZ-225		FortiAnalyzer-VM64				
root						
FCTEMS0000116009	10.3.120.241	FortiClient-EMS	Real Time	N/A	0%	
root		vdom	Real Time	N/A	0%	
FGT61F-V64	10.2.60.43	FortiGate-61F	Real Time	N/A	0%	
root		vdom	Real Time	N/A	0%	
FGT91E-3	10.2.60.250	FortiGate-91E	Real Time	N/A	0%	
root		vdom	Real Time	N/A	0%	
vd1		vdom	Real Time	N/A	0%	

## Add LLDP support on FMG and FAZ - 7.2.1

Using the CLI, the link layer discovery protocol (LLDP) feature can be enabled on FortiAnalyzer ports to advertise the device identity and make it discoverable by other devices on the local network segment. After enabling the LLDP feature on a port, the port sends LLDP packets every 30 seconds.



The LLDP feature is set to `disable` by default.

### To enable the LLDP feature:

1. In the CLI, enter the following command:

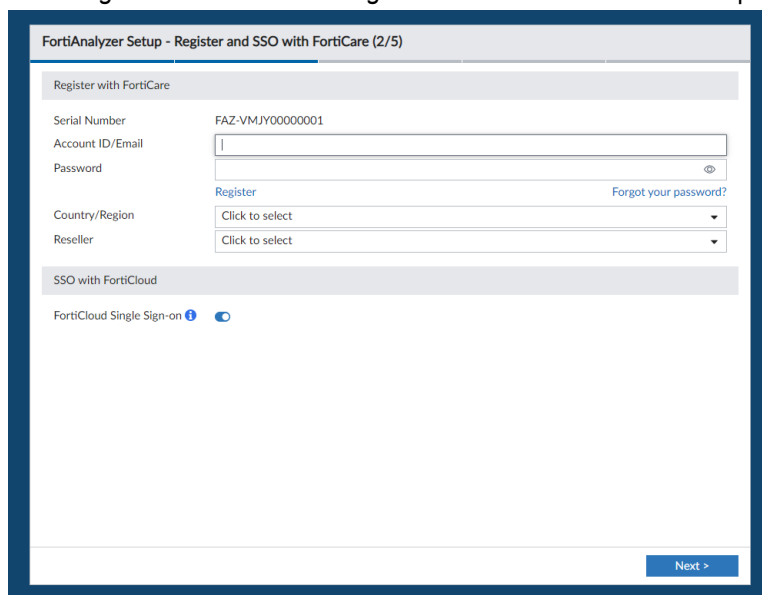
```
config system interface
edit port1
set lldp enable
next
end
```

## Mandatory FortiCare/FortiCloud registration - 7.2.1

Starting in FortiAnalyzer v7.2.1, the administrator must complete the registration process via FortiCare/FortiCloud to use the FortiAnalyzer unit.

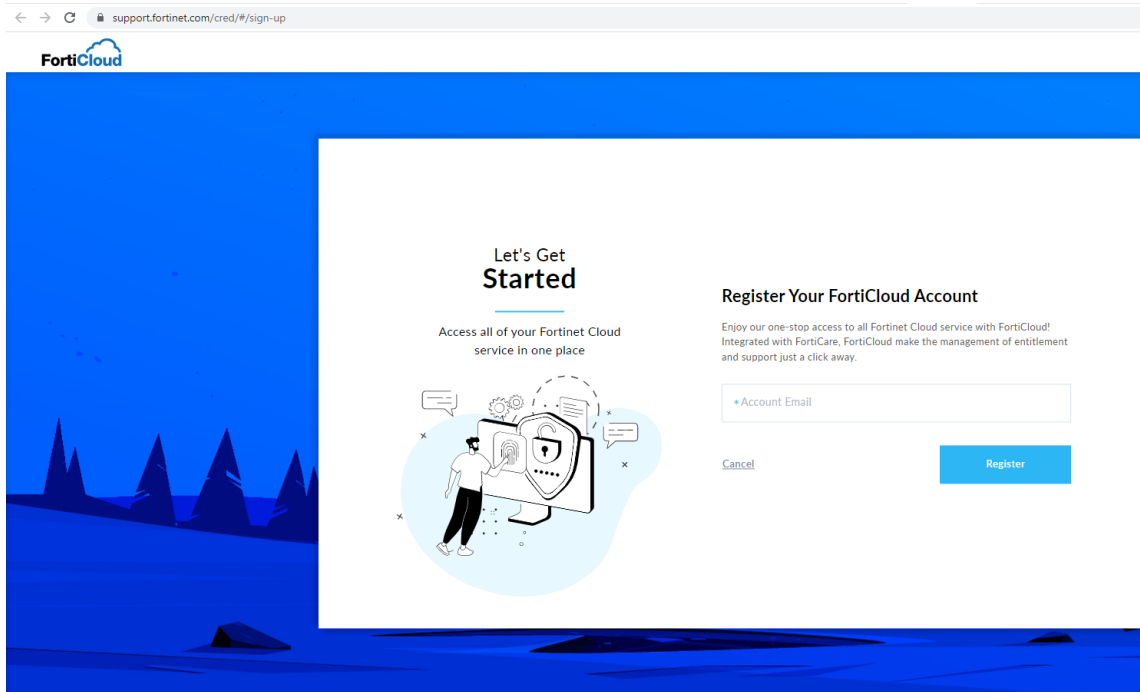
### To complete the mandatory FortiCare registration:

1. Log into the GUI for the new FortiAnalyzer hardware or virtual device.  
The *FortiAnalyzer Setup* wizard displays.
2. Click *Begin* to continue to the *Register and SSO with FortiCare* step.



3. Click **Register**.

The FortiCare website opens, prompting you to register the FortiAnalyzer device.



4. After completing the registration, fill in the required information in the GUI.

A screenshot of the 'FortiAnalyzer Setup - Register and SSO with FortiCare (2/5)' screen. The screen is divided into two main sections: 'Register with FortiCare' and 'SSO with FortiCloud'. The 'Register with FortiCare' section contains the following fields: 'Serial Number' (FAZ-VMJY00000001), 'Account ID/Email' (test@test.com), 'Password' (masked with dots), 'Country/Region' (Canada), and 'Reseller' (Click to select). There are 'Register' and 'Forgot your password?' links. The 'SSO with FortiCloud' section has a 'FortiCloud Single Sign-on' toggle switch which is currently turned on. A blue 'Next >' button is located at the bottom right of the screen.

5. Click **Next** and complete the remaining steps in the *FortiAnalyzer Setup* wizard.

The next time the admin logs in, the *Register and SSO with FortiCare* step will no longer be required.

# Cloud Services

This section lists the new features added to FortiAnalyzer for cloud services:

- FortiAnalyzer management from FortiGate Cloud 7.2.1 on page 111
- VM flexible shapes support for Oracle Cloud Infrastructure 7.2.1 on page 113
- FortiAnalyzer-VM has been added to the Flex-VM offering 7.2.2 on page 115
- FortiAnalyzer-VM supported in OCI DRCC 7.2.2 on page 116

## FortiAnalyzer management from FortiGate Cloud - 7.2.1

FortiAnalyzer can now be managed from the FortiGate Cloud.

Your FortiAnalyzer device must be registered with FortiCloud.

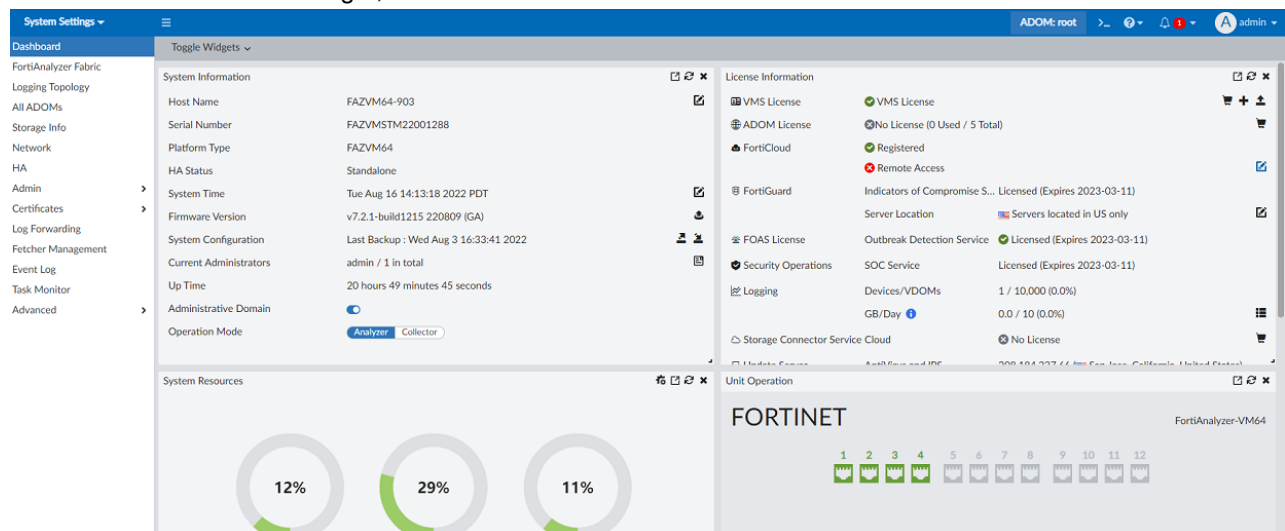


You cannot enable remote access from FortiCloud if the FortiAnalyzer is managed by a FortiManager. You must disable the management before enabling remote access.

For a FortiAnalyzer high availability (HA) cluster, each member should independently register to FortiCloud. However, only the primary unit can enable remote access from FortiCloud.

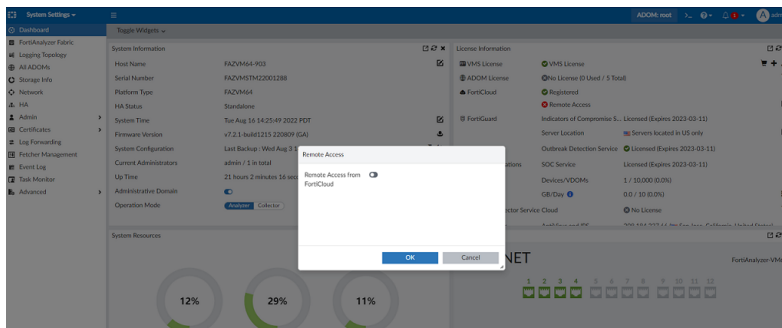
**To enable remote access from FortiCloud using the GUI:**

1. Go to *System Settings > Dashboard*.
2. In the *License Information* widget, click the edit icon for *Remote Access*.

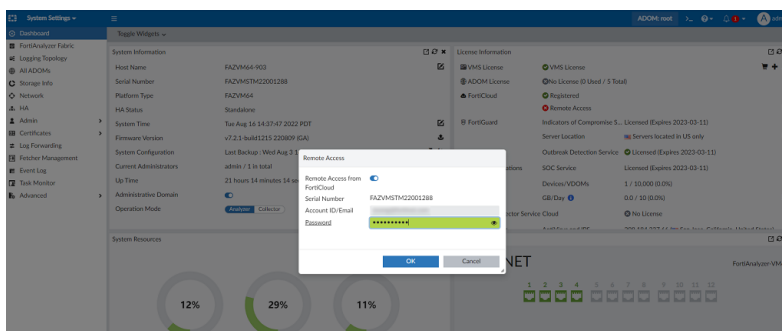


The *Remote Access* dialog opens.

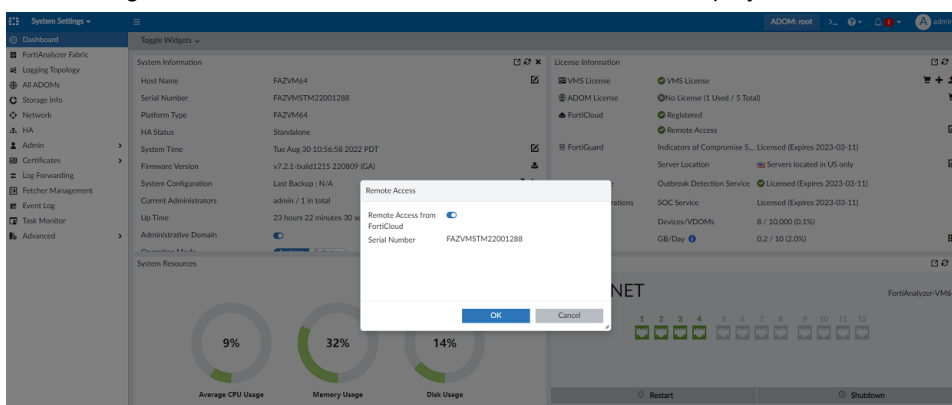
### 3. Enable *Remote Access from FortiCloud*.



4. In the *Password* field, enter the FortiCloud password.  
The *Serial Number* and *FortiCloud Account ID/Email* are automatically populated.
5. Click *OK*.



After the login is successful, *Remote Access from FortiCloud* displays as enabled.



### To enable remote access from FortiCloud using the CLI:

1. In the FortiAnalyzer CLI, enter the following command:  

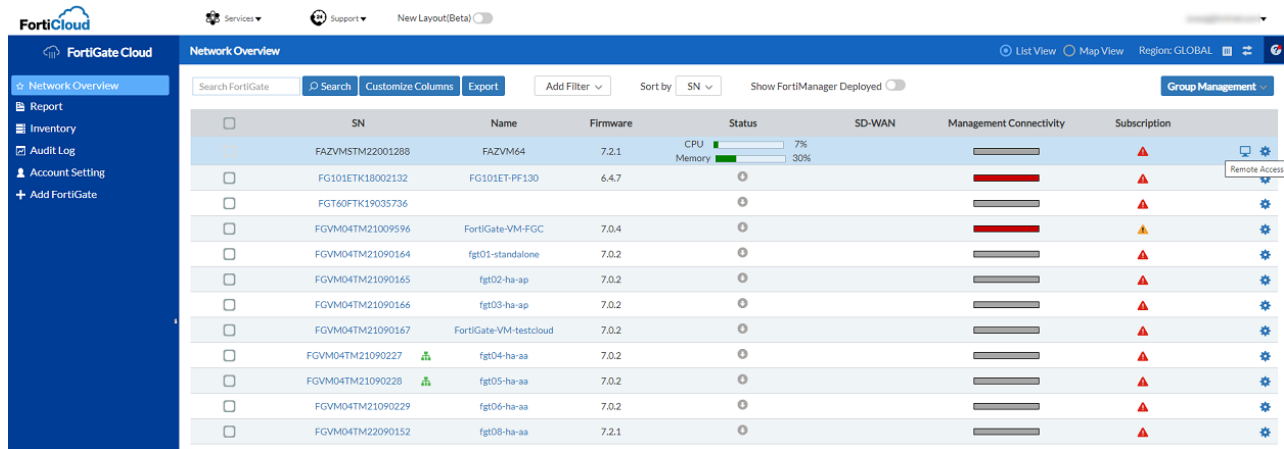
```
config system central-management
set type fortigatecloud
end
```
2. In the FortiAnalyzer CLI, enter the following command:  

```
execute cloud-remote-access login <account-id> <password>
```

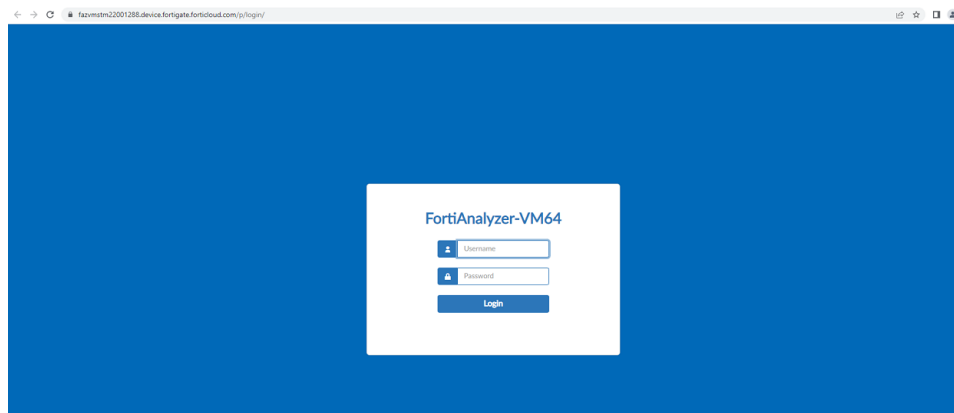


### To use remote access from FortiCloud:

1. Log in to [FortiCloud](#).
2. Go to *Network Overview*.
3. In the row for the enabled FortiAnalyzer device, click the *Remote Access* icon.



The login page for the FortiAnalyzer displays.



## VM flexible shapes support for Oracle Cloud Infrastructure - 7.2.1

The VM flexible shapes now supported for Oracle Cloud Infrastructure (OCI) permit customization for OCPU and memory resources.

When you create a VM instance using a flexible shape, you can select the number of OCPUs and the amount of memory that you need for the workloads that run on the instance. The network bandwidth and number of VNICs scale proportionately with the number of OCPUs.

For more information about instance type support, see the [FortiAnalyzer OCI Administration Guide](#).

When creating a FortiManager-VM or FortiAnalyzer-VM instance in OCI, you can select one of the following flexible shapes:

- VM.Standard3.Flex (Intel)

### Create compute instance


**Image and shape**

A **shape** is a template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance.

Image

v7.2.1

Shape

**VM.Standard3.Flex** 

Virtual machine, 1 core OCPU, 16 GB memory, 1 Gbps network bandwidth

[Show advanced options](#)

**Networking**

Networking is how your instance connects to the internet and other resources in the Console. To

Primary network

[Select existing virtual cloud network](#) [Create new virtual cloud network](#) [Enter subnet ID](#)

[Create](#) [Save as stack](#) [Cancel](#)

### Browse all shapes

A **shape** is a template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance.

Instance type

**Virtual machine**  
A virtual machine is an independent computing environment that runs on top of physical bare metal hardware.

**Bare metal machine**  
A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Shape series

**AMD**  
Flexible OCPU count.  
Current generation AMD processors.

**Intel**  
Flexible OCPU count.  
Current generation Intel processors.

**Ampere**  
Arm-based processor.

**Specialty and previous generation**  
Always Free, Dense I/O, GPU, HPC, and earlier generation AMD and Intel standard shapes.

Image: Custom Custom

Shape name	OCPU	Memory (GB)	Network bandwidth (Gbps)	Max. total VNics
<input checked="" type="checkbox"/> <b>VM.Standard3.Flex</b>	1	16	1	2

You can customize the number of OCPUs and the amount of memory allocated to a flexible shape. The other resources scale proportionately. [Learn more about flexible shapes](#)

Number of OCPUs

1 8 16 24 32 1

☐ Burstable

Amount of memory (GB)

[Select shape](#) [Cancel](#)

- VM.Standard.E3.Flex (AMD)

### Create compute instance


**Image and shape**

A **shape** is a template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance.

Image

v7.2.1

Shape

**VM.Standard.E3.Flex** 

Virtual machine, 1 core OCPU, 16 GB memory, 1 Gbps network bandwidth

[Show advanced options](#)

**Networking**

Networking is how your instance connects to the internet and other resources in the Console. To

Primary network

[Select existing virtual cloud network](#) [Create new virtual cloud network](#) [Enter subnet ID](#)

[Create](#) [Save as stack](#) [Cancel](#)

### Browse all shapes

A **shape** is a template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance.

Instance type

**Virtual machine**  
A virtual machine is an independent computing environment that runs on top of physical bare metal hardware.

**Bare metal machine**  
A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Shape series

**AMD**  
Flexible OCPU count.  
Current generation AMD processors.

**Intel**  
Flexible OCPU count.  
Current generation Intel processors.

**Ampere**  
Arm-based processor.

**Specialty and previous generation**  
Always Free, Dense I/O, GPU, HPC, and earlier generation AMD and Intel standard shapes.

Image: Custom Custom

Shape name	OCPU	Memory (GB)	Network bandwidth (Gbps)	Max. total VNics
<input type="checkbox"/> VM.Standard.E2.1 Micro	1	1	0.48	1
<input checked="" type="checkbox"/> <b>VM.Standard.E3.Flex</b>	1	16	1	2

You can customize the number of OCPUs and the amount of memory allocated to a flexible shape. The other resources scale proportionately. [Learn more about flexible shapes](#)

Number of OCPUs

1 22 43 64 1

☐ Burstable

Amount of memory (GB)

[Select shape](#) [Cancel](#)

- VM.Standard.E4.Flex (AMD)

### Create compute instance


**Image and shape**

A **shape** is a template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance.

Image

v7.2.1

Shape

**VM.Standard.E4.Flex** 

Virtual machine, 1 core OCPU, 16 GB memory, 1 Gbps network bandwidth

[Show advanced options](#)

**Networking**

Networking is how your instance connects to the internet and other resources in the Console. To

Primary network

[Select existing virtual cloud network](#) [Create new virtual cloud network](#) [Enter subnet ID](#)

[Create](#) [Save as stack](#) [Cancel](#)

### Browse all shapes

A **shape** is a template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance.

Instance type

**Virtual machine**  
A virtual machine is an independent computing environment that runs on top of physical bare metal hardware.

**Bare metal machine**  
A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Shape series

**AMD**  
Flexible OCPU count.  
Current generation AMD processors.

**Intel**  
Flexible OCPU count.  
Current generation Intel processors.

**Ampere**  
Arm-based processor.

**Specialty and previous generation**  
Always Free, Dense I/O, GPU, HPC, and earlier generation AMD and Intel standard shapes.

Image: Custom Custom

Shape name	OCPU	Memory (GB)	Network bandwidth (Gbps)	Max. total VNics
<input checked="" type="checkbox"/> <b>VM.Standard.E4.Flex</b>	1	16	1	2

You can customize the number of OCPUs and the amount of memory allocated to a flexible shape. The other resources scale proportionately. [Learn more about flexible shapes](#)

Number of OCPUs

1 22 43 64 1

☐ Burstable

Amount of memory (GB)

[Select shape](#) [Cancel](#)

When creating an instance with a flexible shape, you can use the horizontal scrolls to customize the *Number of OCPUs* and the *Amount of memory (GB)*.



VM BYOL licenses are based on vCPUs. The minimum vCPU support for FortiManager-VM and FortiAnalyzer-VM is 4. 1 OCPU equates to 2 vCPUs. Ensure that you meet the requirements for your license.

Once the instance is created, you can check the instance shape from the dashboard as well. For example, see the dashboard for a VM.Standard3.Flex (Intel) shape below.

**General information**

Availability domain: AD-1  
 Fault domain: FD-2  
 Region: iad  
 OCID: ...nek36q [Show](#) [Copy](#)  
 Launched: Mon, Jul 4, 2022, 17:10:04 UTC  
 Compartment: fortinetoracled1 (root)  
 Capacity type: On-demand

**Instance details**

Virtual cloud network: [hkalga-vcn](#)  
 Maintenance reboot: -  
 Image: [v7.2.1](#)  
 Launch mode: EMULATED  
 Instance metadata service: Versions 1 and 2 [Edit](#) ⓘ  
 Live migration: Use recommended default ⓘ  
 Maintenance recovery action: Restore instance

**Shape configuration**

Shape: VM.Standard3.Flex  
 OCPU count: 16  
 Network bandwidth (Gbps): 16  
 Memory (GB): 256  
 Local disk: Block storage only

**Instance access**

We're not quite sure how to connect to an instance that uses this image. Refer to the image's documentation, or see the general steps to [connect to a running instance](#).

Public IP address: [Copy](#)

**Primary VNIC**

Private IP address: [Copy](#)  
 Network security groups: None [Edit](#) ⓘ  
 Subnet: [My Subnet](#)  
 Private DNS record: Enable  
 Hostname: instance-20220704-1007  
 Internal FQDN: instance-20220704-1007... [Show](#) [Copy](#)

**Launch options**

NIC attachment type: E1000  
 Remote data volume: SCSI  
 Firmware: BIOS  
 Boot volume type: IDE  
 In-transit encryption: Disabled  
 Secure Boot: Disabled  
 Measured Boot: Disabled  
 Trusted Platform Module: Disabled

With this flexible shape, you can customize the number of OCPUs and the amount of memory when launching or resizing your VM.

## FortiAnalyzer-VM has been added to the Flex-VM offering - 7.2.2

FortiAnalyzer-VM has been added to the Flex-VM offering. This allows you to scale the daily storage and number of ADOMs according to your need.

For additional information, see the [Flex-VM Administration Guide](#) on the Fortinet Documents library.

### To activate the Flex-VM token:

1. In Flex-VM, configure the FortiAnalyzer Flex-VM device, including the daily storage and number of ADOMs.

**FortiCloud** Manage Configuration

**4. Complete**

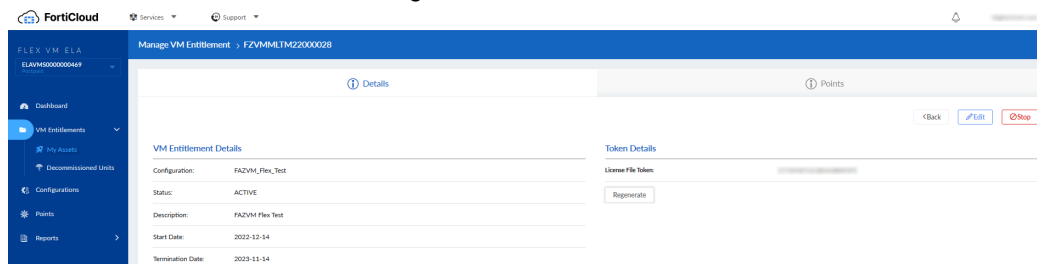
**SUCCESS!**  
Configuration created successfully.

**Configuration Details**

FortiAnalyzer Virtual Machine	
Name	FA2VM_Flex_Test
Status	ACTIVE
Program Serial Number	ELAVM50000000469
Daily Storage (GB)	5
Number of ADOMs	0
Support Services	FortiCare Premium

[List](#) [New Configuration](#)

2. In Flex-VM, add a VM entitlement to get a license file token.



3. Using the FortiAnalyzer Flex-VM token, enter the following command in the FortiAnalyzer CLI to activate the license:

```
execute vm-license <license-token>
```

4. FortiAnalyzer will retrieve the license from Flex-VM, including the daily storage and number of ADOMs.

License Information			
VMS License	Flex-VM License		
ADOM License	Valid until 2025-02-14 (0 Used / 6 Total)		
FortiCloud	Registered	Cloud Management	
FortiGuard	Indicators of Compromise Serv...	Licensed (Expires 2025-02-14)	
	FortiAnalyzer Outbreak Detect...	Licensed (Expires 2025-02-14)	
	Server Location	Servers located in US only	
Security Operations	Security Automation	Licensed (Expires 2025-02-14)	
Logging	Devices/VDOMs	0 / 10,000 (0.0%)	
	GB/Day	0.0 / 6 (0.0%)	
Storage Connector Service	Cloud	No License	
Update Server	AntiVirus and IPS	12.34.97.16 (Ashburn, Virginia, United States)	

## FortiAnalyzer-VM supported in OCI DRCC - 7.2.2

As of FortiAnalyzer 7.2.2, FortiAnalyzer-VM is supported in OCI Dedicated Region Cloud@Customer (DRCC). For more information, see the [FortiAnalyzer OCI Administration Guide](#).

# Index

The following index provides a list of all new features added to FortiAnalyzer 7.2. The index allows you to quickly identify the version where the feature first became available in FortiAnalyzer.

## 7.2.0

- OAuth 2.0 authentication for webhook connectors on page 14
- Network reconnaissance events detection on page 18
- Shadow IT events detection on page 22
- Summary dashboard for event logs on page 58
- Log caching enhancement on page 62
- Add French language support to GUI on page 101
- FortiAnalyzer supports VLANs on physical network interfaces on page 103
- New event handlers for NOC monitoring on page 25
- Report in JSON format on page 69
- Use ServiceNow connector in playbooks on page 16
- Device Group on page 7
- SD-WAN chart to include more ADVPN shortcut information on page 40
- SD-WAN chart for MOS scoring on page 42
- Use device metadata in datasets and reports on page 93
- Search by object names on page 95
- Report cache control on page 70
- Rename Outbreak Alerts Service to Outbreak Detection Service on page 55
- FortiAnalyzer Fabric usability improvements on page 105
- Add ZTNA dashboard to FortiView on page 46
- Include IOC detected on FortiGate local traffic in FortiAnalyzer IOC view on page 27
- IoT visibility on page 49
- Upgrade report editor on page 71
- Improve data visualization for the web usage report on page 74
- 360 Security Report on page 76

## 7.2.1

- Add LLDP support on FMG and FAZ 7.2.1 on page 109
- Global log search across FortiAnalyzer Fabric members 7.2.1 on page 98
- Support for six major versions of FortiOS 7.2.1 on page 10
- FortiNDR logging and reporting enhancements 7.2.1 on page 64
- VPN report update 7.2.1 on page 78

- Security events consolidated page 7.2.1 on page 66
- Traffic shaping charts 7.2.1 on page 50
- Application risk and control report update 7.2.1 on page 82
- Bandwidth and applications report update 7.2.1 on page 84
- Security events and incidents summary report update 7.2.1 on page 85
- High bandwidth application usage report update 7.2.1 on page 87
- Cyber-bullying indicators report update 7.2.1 on page 89
- FortiAnalyzer management from FortiGate Cloud 7.2.1 on page 111
- VM flexible shapes support for Oracle Cloud Infrastructure 7.2.1 on page 113
- CASB Apps Access widget 7.2.1 on page 53
- Mandatory FortiCare/FortiCloud registration 7.2.1 on page 109

## 7.2.2

- Rule based event correlation 7.2.2 on page 28
- Auto-refresh on FortiSoC dashboard elements 7.2.2 on page 54
- Data exfiltration detection 7.2.2 on page 37
- Generate system event log when daemon crashes 7.2.2 on page 96
- Self-harm and risk indicators report update 7.2.2 on page 91
- FortiAnalyzer-VM has been added to the Flex-VM offering 7.2.2 on page 115
- FortiAnalyzer-VM supported in OCI DRCC 7.2.2 on page 116



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.